II

(Atos não legislativos)

DECISÕES

DECISÃO DE EXECUÇÃO (UE) 2016/1250 DA COMISSÃO

de 12 de julho de 2016

relativa ao nível de proteção assegurado pelo Escudo de Proteção da Privacidade UE-EUA, com fundamento na Diretiva 95/46/CE do Parlamento Europeu e do Conselho

[notificada com o número C(2016) 4176]

(Texto relevante para efeitos do EEE)

A COMISSÃO EUROPEIA,

Tendo em conta o Tratado sobre o Funcionamento da União Europeia,

Tendo em conta 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 ([1]), nomeadamente, do artigo 25.º, n.º 6,

Após consulta da Autoridade Europeia para a Proteção de Dados ([2]),

1. INTRODUÇÃO

(1) A Diretiva 95/46/CE estabelece as regras relativas à transferência de dados pessoais dos Estados-Membros para países terceiros, desde que as referidas transferências sejam abrangidas pelo seu âmbito de aplicação.

(2) O artigo 1.º da Diretiva 95/46/CE e os considerandos 2 e 10 do seu preâmbulo pretendem assegurar não apenas a proteção completa e efetiva das liberdades e dos direitos fundamentais das pessoas singulares, nomeadamente o direito fundamental ao respeito pela vida privada no que se refere ao tratamento de dados pessoais, mas também um elevado nível de proteção desses direitos e liberdades fundamentais ([3]).

(3) A importância tanto do direito fundamental ao respeito pela vida privada, garantido pelo artigo 7.º, como do direito fundamental à proteção de dados pessoais, garantido pelo artigo 8.º da Carta dos Direitos Fundamentais da União Europeia, foi salientada na jurisprudência do Tribunal de Justiça ([4]).

(4) Nos termos do artigo 25.º, n.º 1, da Diretiva 95/46/CE, os Estados-Membros devem estabelecer que a transferência de dados pessoais para um país terceiro só pode realizar-se se o país terceiro em questão assegurar um nível de proteção adequado e as legislações dos Estados-Membros que transpõem outras disposições da diretiva tiverem sido respeitadas antes de efetuada a transferência. A Comissão pode considerar que um país terceiro assegura tal nível de proteção adequado em virtude da sua legislação nacional ou dos compromissos internacionais que assumiu a fim de proteger os direitos das pessoas. Nesse caso, e sem prejuízo da observância das disposições nacionais adotadas nos termos de outras disposições da diretiva, os dados pessoais podem ser transferidos dos Estados-Membros sem que sejam necessárias garantias adicionais.

([1]) JO L 281 de 23.11.1995, p. 31.
([2]) Ver Parecer 4/2016 sobre o projeto de decisão relativa ao nível de proteção assegurado pelo Escudo de Proteção da Privacidade UE-EUA, publicada em 30 de maio de 2016.
([3]) Processo C-362/14, *Maximillian Schrems/Data Protection Commissioner* («*Schrems*»), EU:C:2015:650, n.º 39.
([4]) Processo C-553/07, *Rijkeboer*, EU:C:2009:293, n.º 47; Processos apensos C-293/12 e C-594/12, *Digital Rights Ireland e outros*, EU:C:2014:238, n.º 53; Processo C-131/12, *Google Spain e Google*, EU:C:2014:317, n.ºs 53, 66 e 74.

(5) Nos termos do artigo 25.º, n.º 2, da Diretiva 95/46/CE, o nível de proteção dos dados oferecido por um país terceiro deve ser apreciado em função de todas as circunstâncias que rodeiem a transferência ou o conjunto de transferências de dados, em especial, as regras de direito, gerais ou setoriais, em vigor no país terceiro em causa.

(6) Na Decisão 2000/520/CE da Comissão ([5]), para efeitos do artigo 25.º, n.º 2, da Diretiva 95/46/CE, considerou-se que os «princípios da privacidade em porto seguro», aplicados em conformidade com as orientações facultadas pelas denominadas «questões mais frequentes» emitidas pelo *Department of Commerce* (equivalente a Ministério do Comércio) dos Estados Unidos da América, asseguravam um nível de proteção adequado dos dados pessoais transferidos da União para organizações estabelecidas nos Estados Unidos.

(7) Nas suas comunicações COM(2013) 846 final ([6]) e COM(2013) 847 final, de 27 de novembro de 2013 ([7]), a Comissão considerou que os fundamentos essenciais do sistema «porto seguro» deveriam ser reexaminados e reforçados no contexto de vários fatores, nomeadamente o aumento exponencial dos fluxos de dados e a respetiva importância fundamental para a economia transatlântica, o rápido crescimento do número de empresas estabelecidas nos EUA que subscrevem os princípios de «porto seguro» e as novas informações sobre a dimensão e o âmbito de aplicação de determinados programas de informações dos EUA, que levantaram questões quanto ao nível da proteção que o acordo conseguiria garantir. Além disso, a Comissão identificou várias lacunas e deficiências no sistema «porto seguro».

(8) Com base nos elementos de prova recolhidos pela Comissão, designadamente nas informações decorrentes dos trabalhos desenvolvidos pelo grupo de contacto UE-EUA sobre a proteção da vida privada ([8]) e nas informações sobre os programas de informações dos EUA recebidas no grupo de trabalho *ad hoc* UE-EUA ([9]), a Comissão formulou 13 recomendações para uma reapreciação do sistema «porto seguro». Estas recomendações centraram-se no reforço dos princípios materiais de proteção da privacidade, através no aumento da transparência das políticas de proteção da vida privada das empresas autocertificadas dos EUA, de uma melhor supervisão, do controlo e da aplicação, pelas autoridades dos EUA, da observância desses princípios, da disponibilidade de mecanismos de resolução de litígios acessíveis, e na necessidade de assegurar que a utilização da derrogação por motivos de segurança nacional constante da Decisão 2000/520/CE é proporcionada e se limita ao estritamente necessário.

(9) No seu acórdão de 6 de outubro de 2015 no processo C-362/14, *Maximillian Schrems/Data Protection Commissioner* ([10]), o Tribunal de Justiça da União Europeia declarou inválida a Decisão 2000/520/CE. Sem examinar o conteúdo dos princípios da «privacidade em porto seguro», o Tribunal considerou que a Comissão não havia afirmado nessa decisão que os Estados Unidos «asseguravam» efetivamente um nível de proteção adequado em virtude da sua legislação interna ou dos seus compromissos internacionais ([11]).

(10) A este respeito, o Tribunal de Justiça explicou que, embora o termo «nível de proteção adequado» expresso no artigo 25.º, n.º 6, da Diretiva 95/46/CE não implique um nível de proteção idêntico ao garantido na ordem jurídica da União, deve ser entendido no sentido de exigir que esse país terceiro assegure um nível de proteção das liberdades e dos direitos fundamentais «substancialmente equivalente» ao conferido na União nos termos da Diretiva 95/46/CE, lida à luz da Carta dos Direitos Fundamentais. Ainda que, a este respeito, os meios a que esse país recorre possam ser diferentes dos implementados dentro da União, tais meios devem, todavia, revelar-se efetivos, na prática ([12]).

(11) O Tribunal de Justiça criticou a ausência de constatações suficientes na Decisão 2000/520/CE relativamente à existência, nos Estados Unidos da América, de normas de caráter estadual destinadas a limitar as eventuais ingerências nos direitos fundamentais das pessoas cujos dados sejam transferidos da União para os Estados Unidos, ingerências essas que as autoridades estaduais deste país seriam autorizadas a praticar quando prosseguem objetivos legítimos, tais como a segurança nacional, bem como à existência de uma proteção jurídica eficaz contra ingerências desta natureza ([13]).

([5]) 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* (equivalente a Ministério do Comércio) dos Estados Unidos da América (JO L 215 de 28.8.2000, p. 7).

([6]) Comunicação da Comissão ao Parlamento Europeu e ao Conselho Restabelecer a confiança nos fluxos de dados entre a UE e os EUA, COM(2013) 846 final de 27 de novembro de 2013.

([7]) Comunicação da Comissão ao Parlamento Europeu e ao Conselho sobre o funcionamento do sistema «porto seguro» na perspetiva dos cidadãos da UE e das empresas estabelecidas na UE, COM(2013) 847 final de 27 de novembro de 2013.

([8]) Ver, por exemplo, Conselho da União Europeia, relatório final do grupo de contacto de alto nível UE-EUA sobre o intercâmbio de informações e a proteção da vida privada e dos dados pessoais, Nota 9831/08, 28 de maio de 2008, disponível na Internet em: http://www.europarl.europa.eu/document/activities/cont/201010/20101019ATT88359/20101019ATT88359EN.pdf

([9]) Relatório sobre as conclusões dos copresidentes da UE do grupo de trabalho *ad hoc* UE-EUA sobre proteção de dados, 27.11.2013, disponível na Internet em: http://ec.europa.eu/justice/data-protection/files/report-findings-of-the-ad-hoc-eu-us-working-group-on-data-protection.pdf

([10]) Ver nota de rodapé 3.

([11]) *Schrems*, n.º 97.

([12]) *Schrems*, n.ºs 73 e 74.

([13]) *Schrems*, n.ºs 88 e 89.

(12) Em 2014, a Comissão tinha encetado conversações com as autoridades dos EUA a fim de debater o reforço do sistema «porto seguro» em conformidade com as 13 recomendações apresentadas na Comunicação COM(2013) 847 final. Após o acórdão do Tribunal de Justiça da União Europeia no processo *Schrems*, verificou-se uma intensificação do diálogo, com vista a alcançar uma eventual nova decisão de adequação que preenchesse os requisitos do artigo 25.º da Diretiva 95/46/CE, tal como interpretado pelo Tribunal de Justiça. Os documentos que figuram em anexo à presente decisão e que também serão publicados no Registo Federal dos Estados Unidos constituem o resultado destes debates. Os princípios de privacidade (anexo II), em conjunto com os compromissos e as declarações oficiais de várias autoridades dos EUA constantes dos documentos nos anexos I e III a VII, constituem o «Escudo de Proteção da Privacidade UE-EUA».

(13) A Comissão analisou cuidadosamente a legislação e a prática dos EUA, nomeadamente estes compromissos e declarações oficiais. Com base nas conclusões estabelecidas nos considerandos (136)-(140), a Comissão conclui que os EUA asseguram um nível de proteção adequado dos dados pessoais transferidos ao abrigo do Escudo de Proteção da Privacidade UE-EUA da União para organizações autocertificadas nos Estados Unidos.

2. **O «ESCUDO DE PROTEÇÃO DA PRIVACIDADE UE-EUA»**

(14) O Escudo de Proteção da Privacidade UE-EUA baseia-se num sistema de autocertificação através do qual as organizações dos EUA assumem o compromisso de estabelecer um conjunto de princípios de privacidade — os princípios do quadro do Escudo de Proteção da Privacidade UE-EUA, incluindo os princípios suplementares (em seguida designados em conjunto «os princípios») — emitidos pelo *Department of Commerce* dos EUA e constantes do anexo II da presente decisão. É aplicável simultaneamente aos responsáveis pelo tratamento e aos subcontratantes (agentes), com a especificidade de que os subcontratantes devem ser contratualmente obrigados a agir apenas mediante instruções do responsável europeu pelo tratamento e ajudar este último a responder aos pedidos das pessoas que exercem os seus direitos por força destes princípios ([14]).

(15) Sem prejuízo do respeito das disposições nacionais adotadas em aplicação da Diretiva 95/46/CE, a presente decisão tem por efeito autorizar as transferências de um responsável pelo tratamento ou de um subcontratante da União para organizações americanas que autocertificaram a sua adesão aos princípios junto do *Department of Commerce* e que se comprometeram a respeitá-los. Os princípios só se aplicam ao tratamento dos dados pessoais pela organização americana, na medida em que esse tratamento não seja abrangido pelo âmbito de aplicação da legislação da União ([15]). O Escudo de Proteção da Privacidade não prejudica a aplicação da legislação da União que rege o tratamento dos dados pessoais nos Estados-Membros ([16]).

([14]) Ver a secção III.10.a. do anexo II. Em conformidade com a definição dada na secção I.8.c, o responsável europeu pelo tratamento determinará a finalidade e os meios do tratamento dos dados pessoais. Além disso, o contrato celebrado com o agente deve indicar claramente se são autorizadas transferências posteriores (ver secção III.10.a. ii.2.).

([15]) Tal é igualmente aplicável em relação aos dados relativos aos recursos humanos transferidos a partir da União no contexto de uma relação de trabalho. Embora os princípios sublinhem a «principal responsabilidade» do empregador da UE (ver secção III.9.d.i. do anexo II), indicam claramente que o comportamento deste último será abrangido pelas regras aplicáveis na União e/ou no Estado-Membros em causa, não pelos princípios. Ver as secções III.9.a.i., b.ii., c.i. e d.i. do anexo II.

([16]) As mesmas regras são aplicáveis igualmente aos tratamentos efetuados através da utilização de equipamentos situados na União, mas utilizados por uma organização situada fora da União (ver o artigo 4.º, n.º 1, alínea c), da Diretiva 95/46/CE). A partir de 25 de maio de 2018, o Regulamento Geral sobre a Proteção de Dados será aplicável i) ao tratamento dos dados pessoais no contexto das atividades de um estabelecimento de um responsável pelo tratamento ou de um subcontratante no território da União (mesmo quando o tratamento é efetuado nos Estados Unidos), ou ii) ao tratamento dos dados pessoais relativos a titulares de dados que se encontram na União por um responsável pelo tratamento ou um subcontratante que não está estabelecido na União quando as atividades de tratamento estão ligadas a) à oferta de bens eu de serviços a essas pessoas, independentemente de ser exigido um pagamento dessas pessoas; ou b) ao acompanhamento do comportamento dessas pessoas, na medida em que se trate de um comportamento que ocorreu na União. Ver o artigo 3.º, n.ºs 1 e 2, do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados) (JO L 119 de 4.5.2016, p. 1).

(16) A proteção proporcionada aos dados pessoais pelo Escudo de Proteção da Privacidade é aplicável a qualquer titular de dados da UE ([17]) cujos dados pessoais foram transferidos a partir da UE para organizações situadas nos Estados Unidos que autocertificaram a sua adesão aos princípios junto do *Department of Commerce*.

(17) Os princípios serão aplicáveis imediatamente após a certificação. A única exceção diz respeito ao princípio de responsabilização pela transferência ulterior, quando a organização que se autocertifica no quadro do Escudo de Proteção da Privacidade desenvolve já relações comerciais com terceiros. Como será certamente necessário algum tempo para pôr essas relações em conformidade com as regras aplicáveis ao abrigo do princípio de responsabilização pela transferência ulterior, a organização será obrigada a fazê-lo o mais depressa possível, e de qualquer modo num prazo de nove meses a contar da autocertificação (desde que esta se realize nos dois meses seguintes ao dia de entrada em vigor do Escudo de Proteção da Privacidade). Durante este período transitório, a organização deve aplicar o princípio de aviso e princípio de escolha (permitindo assim ao titular de dados da UE opor-se ao tratamento) e, quando os dados pessoais forem transferidos para um terceiro agindo na qualidade de agente, deve assegurar-se que este prevê pelo menos o mesmo nível de proteção que é exigido pelos princípios ([18]). Este período transitório prevê um equilíbrio razoável e adequado entre o respeito do direito fundamental de proteção dos dados e a necessidade legítima das empresas disporem de um prazo suficiente para se adaptarem ao novo quadro, nos casos em que tal dependa também das suas relações comerciais com terceiros.

(18) O sistema será administrado e acompanhado pelo *Department of Commerce* com base nos seus compromissos estabelecidos nas declarações do Secretário do Comércio dos EUA (anexo I da presente decisão). No que diz respeito à aplicação dos princípios, a *Federal Trade Commission* (FTC) e o *Department of Transportation* apresentaram declarações que constam do anexo IV e do anexo V da presente decisão.

2.1. *Princípios de privacidade*

(19) No âmbito da sua autocertificação ao abrigo do Escudo de Proteção da Privacidade UE-EUA, as organizações têm de se comprometer a cumprir os princípios ([19]).

(20) No âmbito do *princípio de aviso*, as organizações são obrigadas a fornecer informações aos titulares de dados sobre vários elementos-chave relacionados com o tratamento dos seus dados pessoais (por exemplo, tipo de dados recolhidos, finalidade do tratamento, direito de acesso e escolha, condições de transferência ulterior e responsabilidade). São aplicáveis garantias adicionais, nomeadamente o requisito de as organizações publicarem as respetivas políticas em matéria de proteção da vida privada (refletindo os princípios), bem como de apresentarem ligações para o sítio *web* do *Department of Commerce* (com informações adicionais sobre a autocertificação, os direitos dos titulares de dados e os mecanismos de recursos disponíveis), a lista do Escudo de Proteção da Privacidade (a que se refere o considerando 30) e o sítio *web* de uma entidade adequada de resolução alternativa de litígios.

(21) No âmbito do *princípio de integridade dos dados e limitação dos fins*, os dados pessoais devem limitar-se ao que é relevante para o fim do tratamento, ser fiáveis para a utilização prevista, exatos, completos e atuais. Uma organização não pode tratar dados pessoais de modo incompatível com o fim que motivou a recolha original ou que tenha sido autorizado posteriormente pelo titular dos dados. As organizações devem assegurar que os dados pessoais são fiáveis em relação à utilização prevista, exatos, completos e atuais.

([17]) A presente decisão é relevante para efeitos do EEE. O Acordo sobre o Espaço Económico Europeu («Acordo EEE») prevê a extensão do mercado interno da União Europeia à Islândia, ao Listenstaine e à Noruega. A legislação da União em matéria de proteção dos dados, nomeadamente a Diretiva 95/46/CE, é abrangida pelo Acordo EEE e foi integrada no respetivo anexo XI. O Comité Misto do EEE tem de tomar uma decisão sobre a integração da presente decisão no Acordo EEE. Logo que a presente decisão seja aplicável à Islândia, ao Listenstaine e à Noruega, o Escudo de Proteção da Privacidade UE-EUA abrangerá igualmente estes três países e as referências à UE e aos seus Estados-Membros, que figuram no pacote de medidas correspondente, deverão ser entendidas como incluindo-os.

([18]) Ver a secção III.6.e. do anexo II.

([19]) São aplicáveis regras especiais que proporcionam garantias adicionais aos dados relativos a recursos humanos recolhidos no contexto de emprego, tal como estipulado no princípio suplementar sobre «Dados relativos a recursos humanos» dos princípios de privacidade (ver secção III.9. do anexo II). Por exemplo, os empregadores devem integrar as opções dos trabalhadores em matéria de privacidade mediante a limitação do acesso aos dados pessoais, a garantia do anonimato em relação a certos dados ou a atribuição de códigos ou pseudónimos. Mais importante ainda, as organizações são obrigadas a cooperar e a respeitar o aconselhamento das autoridades europeias responsáveis pela proteção dos dados no que diz respeito a tais dados.

(22) Quando uma nova finalidade (finalidade alterada) é materialmente diferente mas contudo compatível com a finalidade inicial, o *princípio da escolha* confere aos titulares de dados o direito de se oporem ao tratamento. O *princípio da escolha* não se substitui à proibição expressa dos tratamentos incompatíveis ([20]). São aplicáveis ao *marketing* direto ([21]) regras especiais que permitem, de forma geral, uma oposição «a qualquer momento» à utilização dos dados pessoais. No caso de dados sensíveis, as organizações devem, normalmente, obter o consentimento expresso (*opt in*) da pessoa cujos dados foram objeto de tratamento.

(23) Ainda ao abrigo do *princípio de integridade dos dados e limitação dos fins*, só podem ser conservadas informações pessoais sob uma forma que permita identificar uma pessoa ou a torne identificável (portanto sob a forma de dados pessoais) enquanto a sua utilização seja conforme à ou às finalidades para as quais foram inicialmente recolhidas ou posterirmente autorizadas. Esta obrigação não impede que as organizações aderentes ao Escudo de Proteção da Privacidade continuem a tratar informações pessoais durante períodos mais longos, mas apenas durante, e na medida em que, esse tratamento sirva razoavelmente para uma das finalidades específicas seguintes: arquivamento no interesse público, jornalismo, literatura e arte, bem como investigação histórica e análise estatística. A conservação de dados pessoais durante um período mais longo para uma destas finalidades será sujeita às garantias previstas nos princípios.

(24) No âmbito do *princípio de segurança*, as organizações que criam, mantêm, utilizam ou divulgam dados pessoais devem tomar precauções de segurança «razoáveis e adequadas», tomando em consideração os riscos que o tratamento e a natureza dos dados implicam. No caso de tratamento ulterior, as organizações devem celebrar um contrato com a entidade que procederá ao tratamento ulterior dos dados que assegure o mesmo nível de proteção previsto pelos princípios e tomar medidas para assegurar a sua aplicação adequada.

(25) No âmbito do *princípio de acesso* ([22]), os titulares de dados têm o direito, sem necessidade de justificação e apenas em troca de uma taxa não excessiva, de obter de uma organização a confirmação de se esta trata dados pessoais relacionados consigo e de que os dados lhe sejam comunicados num prazo razoável. Este direito só pode ser limitado em circunstâncias excecionais; qualquer recusa ou limitação do direito de acesso deve ser necessária, devidamente justificada e a organização deve suportar o ónus de demonstrar que estes requisitos são preenchidos. Os titulares de dados devem poder corrigir, alterar ou eliminar informações pessoais sempre que estas sejam incorretas ou tenham sido tratadas em violação dos princípios. Em domínios em que é muito provável que as empresas recorram ao tratamento automatizado de dados pessoais para tomar decisões que afetem a pessoa (por exemplo, concessão de crédito, ofertas de crédito hipotecário, emprego), o direito americano proporciona proteções específicas contra as decisões negativas ([23]). Estes atos preveem normalmente que as pessoas têm o direito de serem informadas das razões específicas subjacentes à decisão (por exemplo, a recusa de concessão de um crédito), de contestar as informações incompletas ou inexatas (bem como confiança em fatores ilegais) e procurar obter reparação. Estas regras oferecem proteções no número de casos provavelmente bastante limitado em que a própria organização aderente ao Escudo de Proteção da Privacidade tomaria as decisões automatizadas ([24]). No entanto, tendo em conta a utilização acrescida do tratamento automatizado (incluindo a definição de perfis) enquanto base para tomar decisões que afetam pessoas na economia digital moderna, trata-se de um domínio que deve ser acompanhado de perto. A fim de facilitar este acompanhamento, foi acordado com as autoridades americanas que será previsto um diálogo sobre a tomada de decisão automatizada, incluindo um intercâmbio sobre as semelhanças e as diferenças das abordagens adotadas pela UE e pelos Estados Unidos na matéria, no quadro da primeiro análise anual, bem como de posteriores análises, se necessário.

([20]) Tal é aplicável a todas as transferências de dados no quadro do Escudo de Proteção da Privacidade, incluindo quando dizem respeito a dados recolhidos no contexto de uma relação de trabalho. Embora uma organização americana autocertificada possa, em princípio, utilizar dados relativos a recursos humanos para outros fins que não uma relação de trabalho (por exemplo, para certas comunicações comerciais) deve respeitar a proibição de tratamento incompatível e deve imperativamente respeitar o *princípio de aviso* e o *princípio de escolha*. A proibição feita à organização americana de aplicar sanções contra o assalariado que expressou a sua escolha, nomeadamente entravar a sua carreira profissional, garantirá que, apesar da relação de subordinação e de dependência inerente, não será exercida qualquer pressão sobre o assalariado, podendo este, por conseguinte, efetuar a sua escolha com total liberdade.

([21]) Ver a secção III.12. do anexo II.

([22]) Ver igualmente o princípio suplementar sobre «Acesso» (Seção III.8 do anexo II).

([23]) Ver, por exemplo, o *Equal Credit Opportunity Act* (ECOA, 15 U.S.C. 1691 e seg.), o *Fair Credit Reporting Act* (FRCA, 15 USC § 1681 e seg.) ou o *Fair Housing Act* (FHA, 42 U.S.C. 3601 e seg.).

([24]) No contexto de uma transferência de dados pessoais recolhidos na UE, a relação contratual com a pessoa (o cliente) será na maior parte dos casos — e, por conseguinte, qualquer decisão baseada num tratamento automatizado será normalmente tomada pelo — com o responsável europeu pelo tratamento, que tem de respeitar as regras da UE em matéria de proteção dos dados. Tal inclui cenários em que o tratamento é realizado por uma organização aderente ao Escudo de Proteção da Privacidade, que age na qualidade de mandatário por conta do responsável europeu pelo tratamento.

(26) No âmbito do *princípio de recurso, aplicação e responsabilidade,* ([25]) as organizações participantes devem proporcionar mecanismos robustos para assegurar a conformidade com os restantes princípios e vias de recurso para todos os titulares de dados cujos dados pessoais tenham sido tratados de modo não conforme, nomeadamente reparações eficazes. Quando uma organização tenha decidido, a título voluntário, autocertificar ([26]) a sua adesão ao Escudo de Proteção da Privacidade UE-EUA, o cumprimento efetivo dos princípios é obrigatório. Para poder continuar a basear-se no Escudo de Proteção da Privacidade para receber dados pessoais da União, as organizações devem proceder anualmente à certificação da sua participação no quadro. As organizações devem também tomar medidas para verificar ([27]) que as suas políticas públicas em matéria de proteção da vida privada são conformes com os princípios de privacidade e são efetivamente cumpridas. Tal pode ser efetuado através de um sistema de autoavaliação, que deve incluir procedimentos internos que assegurem que os trabalhadores recebem formação sobre a aplicação das políticas da organização em matéria de proteção da vida privada e que a conformidade é periodicamente reexaminada de forma objetiva, ou verificações de conformidade externas, cujos métodos podem incluir auditorias ou verificações aleatórias. Além disso, a organização deve criar um mecanismo de recurso efetivo para tratar eventuais queixas (ver igualmente a este respeito o considerando 43) e estar sujeita aos poderes de investigação e de execução da FTC, do *Department of Transportation* e de qualquer outro organismo oficial americano que assegurará o respeito efetivo dos princípios.

(27) São aplicáveis regras especiais às transferências designadas como «ulteriores», ou seja, às transferências de dados pessoais de uma organização para um responsável pelo tratamento ou um subcontratante, independentemente de este se encontrar nos Estados Unidos ou num país terceiro fora dos Estados Unidos (e da União). Estas regras têm por objetivo assegurar que a proteção garantida aos dados pessoais dos titulares de dados da UE não será comprometida, e não pode ser contornada, ao transferir esses dados para terceiros. São particularmente importantes em cadeias de tratamento mais complexas, caraterísticas da economia digital atual.

(28) Por força do *princípio de responsabilização pela transferência ulterior* ([28]), qualquer transferência ulterior só pode realizar-se i) para fins limitados e específicos, ii) com base num contrato (ou num dispositivo comparável em caso de transferência no âmbito de um grupo de empresas ([29])) e iii) se nesse contrato estiver previsto o mesmo nível de proteção que o garantido pelos princípios, o que inclui a obrigação de só limitar a aplicação dos princípios na medida do necessário para efeitos da segurança nacional, da aplicação da lei ou de outros interesses públicos ([30]). Estas regras devem ser lidas em conjugação com o *princípio de aviso* e, em caso de transferência posterior para um responsável pelo tratamento num país terceiro ([31]), com o *princípio da escolha*, segundo o qual os titulares de dados devem ser informados (entre outras) do tipo/identidade de qualquer destinatário terceiro, da finalidade da transferência ulterior, bem como da escolha que podem proporcionar e da possibilidade de poderem opor-se (*opt out*) ou, no caso de dados sensíveis, terem de dar «o seu consentimento expresso» (*opt in*) a essas transferências posteriores. Tendo em conta o princípio de integridade dos dados e limitação dos fins, a obrigação de fornecer o mesmo nível de proteção que o garantido pelos princípios, pressupõe que o terceiro só pode tratar as informações pessoais que lhe foram transmitidas para fins que não sejam incompatíveis com os as finalidades para as quais foram inicialmente recolhidos ou posteriormente autorizados pelo titular dos dados.

(29) A obrigação de fornecer o mesmo nível de proteção que o garantido pelos princípios é aplicável a todos os terceiros que intervenham no tratamento dos dados assim transferidos independentemente da sua localização (nos EUA ou num outro país terceiro), bem como quando o destinatário terceiro inicial comunica por sua vez esses dados a um outro destinatário terceiro, por exemplo, para fins de subcontratação. De qualquer modo, o contrato com o destinatário terceiro deve prever que, se este último verificar que deixou de estar em condições de cumprir esta obrigação, informará do facto a organização aderente ao Escudo de Proteção da Privacidade.

([25]) Ver igualmente o princípio suplementar «Resolução de litígios e aplicação» (Secção III.11. do anexo II).
([26]) Ver igualmente o princípio suplementar «Autocertificação» (Seção III.6 do anexo II).
([27]) Ver igualmente o princípio suplementar «Verificação» (Seção III.7 do anexo II).
([28]) Ver igualmente o princípio suplementar «Contratos obrigatórios para as transferências posteriores» (Secção III.10. do anexo II).
([29]) Ver igualmente o princípio suplementar «Contratos obrigatórios para as transferências posteriores» (Secção III.10.b do anexo II). Embora este princípio autorize igualmente transferências que assentem em instrumentos não contratuais (por exemplo, programas de conformidade e controlo intragrupo), o texto indica claramente que esses instrumentos devem sempre «garantir a continuidade da proteção das informações pessoais em conformidade com os princípios». Além disso, dado que a organização americana autocertificada continuará a ser responsável pelo respeito do princípio, terá todo o interesse em utilizar instrumentos realmente eficazes na prática.
([30]) Ver a secção I.5. do anexo II.
([31]) Os titulares de dados não poderão opor-se quando os dados pessoais são transferidos para um terceiro que age na qualidade de mandatário para desempenhar tarefas por conta e segundo as instruções da organização americana. Contudo, deve ter sido assinado um contrato entre o mandatário e a organização americana, incumbindo a esta última garantir a proteção proporcionada pelos princípios, exercendo os seus poderes de instrução.

Nesse caso, deve pôr termo ao tratamento ou devem ser tomadas outras medidas razoáveis e adequadas para solucionar a situação ([32]). Sempre que surjam problemas de cumprimento na cadeia de (sub)tratamento, a organização aderente ao Escudo de Proteção da Privacidade agindo como responsável pelo tratamento dos dados pessoais deverá provar que não é responsável pela questão que dá origem aos danos; caso contrário deverá assumir a responsabilidade, em conformidade com o *princípio de recurso, aplicação e responsabilidade*. Estão previstas proteções suplementares em caso de transferência posterior para um mandatário terceiro ([33]).

2.2. *Transparência, gestão e supervisão do Escudo de Proteção da Privacidade UE-EUA*

(30) O Escudo de Proteção da Privacidade UE-EUA prevê mecanismos de supervisão e de aplicação destinados a verificar e garantir que as empresas americanas autocertificadas respeitam os princípios e que será resolvida qualquer falha de cumprimento. Estes mecanismos são definidos nos princípios (anexo II) e nos compromissos assumidos pelo *Department of Commerce* (anexo I), pela FTC (anexo IV) e pelo *Department of Transportation (anexo V)*.

(31) Para que o Escudo de Proteção da Privacidade UE-EUA seja corretamente aplicado, as partes interessadas, tal como os titulares dos dados, os exportadores de dados e as autoridades nacionais responsáveis pela proteção dos dados devem estar em condições de identificar as organizações aderentes aos princípios. Para o efeito, o *Department of Commerce* assumiu a responsabilidade de manter atualizada e disponibilizar ao público uma lista das organizações que autocertificaram a sua adesão aos princípios e que estão abrangidas pelo âmbito de competência de, pelo menos, uma das autoridades de execução referidas nos anexos I e II da presente decisão («lista do Escudo de Proteção da Privacidade») ([34]). O *Department of Commerce* atualizará a lista com base nos pedidos de renovação da certificação anual das organizações e sempre que uma organização se retire ou seja suprimida do Escudo de Proteção da Privacidade UE-EUA. Também conservará e disponibilizará ao público um registo oficial das organizações suprimidas da lista que, em cada caso, identifica o motivo de tal supressão. Por último, fornecerá uma ligação para a lista de processos da FTC relacionados com a aplicação do Escudo de Proteção da Privacidade conservados que figurará no sítio *web* da FTC.

(32) O *Department of Commerce* publicará a lista do Escudo de Proteção da Privacidade e as declarações de renovação da certificação num sítio *web* específico. As organizações autocertificadas deverão, por seu lado, fornecer o endereço *web* do *Department* para a lista do Escudo de Proteção da Privacidade. Além disso, caso se encontre disponível em linha, a política das organizações em matéria de proteção da vida privada deve incluir uma hiperligação para o sítio *web* do Escudo de Proteção da Privacidade, bem como uma ligação para o sítio *web* ou para um formulário de apresentação de queixas do mecanismo de recurso independente que está disponível para investigar queixas por resolver. O *Department of Commerce* verificará sistematicamente, no contexto da certificação e renovação da certificação da adesão de uma organização ao quadro, se as suas políticas em matéria de proteção da vida privada observam os princípios.

(33) As organizações que tenham persistido em não cumprir os princípios serão suprimidas da lista do Escudo de Proteção da Privacidade e devem devolver ou eliminar os dados pessoais recebidos ao abrigo do Escudo de Proteção da Privacidade UE-EUA. Noutros casos de supressão, tais como a retirada voluntária ou a não renovação da certificação, a organização pode manter os referidos dados se confirmar anualmente ao *Department of Commerce* o seu compromisso de continuar a aplicar os princípios ou proporcionar uma proteção adequada dos dados pessoais através de outros meios autorizados (por exemplo, através de um contrato que reflita na íntegra os requisitos das cláusulas contratuais-tipo relevantes aprovadas pela Comissão). Neste caso, as organizações devem identificar um ponto de contacto na organização para o esclarecimento de todas as questões relacionadas com o Escudo de Proteção da Privacidade.

(34) Além disso, o *Department of Commerce* procederá ao controlo das organizações que já não participam no Escudo de Proteção da Privacidade UE-EUA, quer por se terem retirado voluntariamente ou por a sua certificação ter caducado, a fim de verificar se devolverão, eliminarão ou manterão ([35]) os dados pessoais previamente recebidos

([32]) A situação é diferente consoante o terceiro seja um responsável pelo tratamento ou um subcontratante (mandatário). No primeiro cenário, o contrato celebrado com o terceiro deve prever que este ponha termo ao tratamento ou tome outras medidas razoáveis ou adequadas para remediar a situação. No segundo cenário, incumbe à organização participante no Escudo de Proteção da Privacidade — enquanto organização responsável pelo tratamento, atuando o mandatário sob as suas instruções — tomar essas medidas.

([33]) Nesse caso, a organização americana deve igualmente tomar medidas razoáveis e adequadas i) para garantir que o mandatário trata efetivamente as informações pessoais que lhe são transferidas de forma compatível com as obrigações que incumbem à organização por força dos princípios e ii) para pôr termo e remediar o tratamento não autorizado, logo que seja notificada.

([34]) Para mais informações sobre a gestão da lista do Escudo de Proteção da Privacidade, ver os anexos I e II (Secções I.3, I.4, III.6.d, e III.11.g).

([35]) Ver, por exemplo, secções I.3, III.6.f. e III.11.g.i. do anexo II.

no âmbito do quadro. Se mantiverem estes dados, as organizações são obrigadas a aplicar-lhes os princípios. Nos casos em que o *Department of Commerce* tenha afastado organizações do quadro devido ao incumprimento persistente dos princípios, esta entidade certificar-se-á de que as referidas organizações devolvem ou eliminam os dados pessoais recebidos no âmbito do quadro.

(35) Sempre que, por algum motivo, uma organização abandone o Escudo de Proteção da Privacidade UE-EUA, esta deve eliminar todas as declarações públicas que sugiram que continua a participar no mesmo ou que tem direito aos seus benefícios, nomeadamente quaisquer referências ao Escudo de Proteção da Privacidade UE-EUA na sua política pública em matéria de proteção da vida privada. O *Department of Commerce* procurará e resolverá as falsas declarações de participação no Escudo, incluindo por parte de antigos participantes ([36]). Todas as falsas declarações destinadas ao grande público relativamente à adesão aos princípios sob a forma de declarações ou práticas enganosas são passíveis de medidas de execução pela FTC, pelo *Department of Transportation* ou por outras autoridades de execução americanas; as declarações falsas prestadas ao *Department of Commerce* são passíveis de execução ao abrigo do *False Statements Act* (legislação sobre falsas declarações — 18 USC § 1001) ([37]).

(36) O *Department of Commerce* controlará sistematicamente todas as falsas declarações de participação no Escudo de Proteção da Privacidade ou a utilização indevida da marca de certificação do Escudo de Proteção da Privacidade e as APD podem remeter organizações para um ponto de contacto específico do *Department of Commerce* para efeitos de análise. Sempre que uma organização tenha deixado de participar no Escudo de Proteção da Privacidade UE-EUA, não tenha procedido à renovação da certificação ou seja suprimida da lista do Escudo de Proteção da Privacidade, o *Department of Commerce* verificará, numa base contínua, se esta eliminou da sua política pública em matéria de proteção da vida privada todas as referências ao Escudo de Proteção da Privacidade que sugiram a continuação da sua participação e, caso esta continue a prestar falsas declarações, submeterá a questão à FTC, ao *Department of Transportation* ou a outra autoridade competente para possíveis medidas de execução. Também enviará questionários às organizações cuja autocertificação tenha caducado ou que se tenham voluntariamente retirado do Escudo de Proteção da Privacidade UE-EUA a fim de verificar se as organizações devolverão, eliminarão ou continuarão a aplicar os princípios de privacidade aos dados pessoais que receberam durante a sua participação no Escudo de Proteção da Privacidade e, caso os dados pessoais sejam conservados, verificar quem, no seio da organização, será o ponto de contacto permanente para o esclarecimento de questões relacionadas com o Escudo de Proteção da Privacidade.

(37) Numa base contínua, o *Department of Commerce* realizará análises de conformidade sistemáticas ([38]) das organizações autocertificadas, nomeadamente através do envio de questionários pormenorizados. Também procederá a verificações sistemáticas sempre que tenha recebido uma queixa específica (não abusiva), se uma organização não apresentar respostas válidas às suas questões, ou se existirem indícios credíveis de que uma organização não respeita os princípios. Se necessário, o *Department of Commerce* consultará igualmente as APD em relação às análises de conformidade.

2.3. *Mecanismo de recurso, tratamento de queixas e execução*

(38) O Escudo de Proteção da Privacidade UE-EUA, através do *princípio de recurso, aplicação e responsabilidade*, exige que as organizações criem vias de recurso em caso de incumprimento dos princípios e, por conseguinte, a possibilidade, para os titulares de dados da UE, de apresentarem queixas por incumprimento dos princípios por parte das empresas americanas autocertificadas, e de aquelas serem resolvidas, se necessário mediante uma decisão de reparação efetiva.

(39) No quadro da sua autocertificação, as organizações devem satisfazer os requisitos do princípio de recurso, aplicação e responsabilidade, prevendo mecanismos de recurso independentes facilmente acessíveis e eficazes, através dos quais as queixas e os litígios possam ser examinados e resolvidos sem custos para os titulares de dados.

(40) As organizações podem escolher mecanismos de recurso independentes na União ou nos Estados Unidos, opção que inclui a possibilidade de se comprometer, numa base voluntária, a cooperar com as autoridades responsáveis pela proteção de dados (APD) da UE. Todavia, uma tal escolha não existe quando as organizações tratam dados

([36]) Ver anexo I, secção sobre «Procura e Resolução de falsas declarações de participação».
([37]) Ver as Secções III.6.h. e III.11.f. do anexo II.
([38]) Ver o anexo I.

relativos aos recursos humanos, uma vez que nesse caso a cooperação com as APD é obrigatória. Outras alternativas consistem em recorrer a um organismo independente de resolução alternativa de litígios ou a *programas de proteção da privacidade* elaborados pelo setor privado, que integram os princípios nas suas regras. Estes devem incluir mecanismos de execução eficazes conformes aos requisitos do princípio de recurso, aplicação e responsabilidade. As organizações são obrigadas a solucionar os problemas de não conformidade. Devem igualmente especificar que estão sujeitas aos poderes de investigação e de execução da FTC, do *Department of Transportation* ou de qualquer outro organismo oficial americano.

(41) Por conseguinte, o quadro do Escudo de Proteção da Privacidade fornece aos titulares de dados um certo número de possibilidades para fazerem valer os seus direitos, apresentarem queixas em caso de incumprimento pelas empresas autocertificadas americanas e de aquelas serem resolvidas, se necessário mediante uma decisão de reparação efetiva. Os titulares de dados podem apresentar uma queixa diretamente junto de uma organização, de um organismo independente de resolução de litígios designado pela organização, das APD nacionais ou da FTC.

(42) Nos casos em que essas queixas não foram resolvidas por um desses mecanismos de recurso ou de aplicação, as pessoas têm igualmente o direito de invocar uma arbitragem vinculativa ao abrigo do Comité do Escudo de Proteção da Privacidade (anexos I e II da presente decisão). Salvo no que diz respeito ao comité de arbitragem, que exige o esgotamento de um certo número de vias de recurso antes de se poder recorrer a ele, os titulares de dados têm a liberdade de recorrer a um, a vários ou a todos os mecanismos de recurso da sua escolha, não sendo a obrigados a escolher um determinado mecanismo ou a seguir uma determinada ordem. No entanto, tal como seguidamente mencionado, existe uma certa ordem lógica que é aconselhável seguir.

(43) Em primeiro lugar, os titulares de dados da UE podem recorrer em casos de incumprimento dos princípios através de contactos diretos com a *empresa autocertificada dos EUA*. A fim de facilitar a resolução, a organização deve instaurar um mecanismo de recurso eficaz para tratar de tais queixas. A política das organizações em matéria de proteção da privacidade deve, por conseguinte, informar claramente as pessoas sobre um ponto de contacto, interno ou externo à organização, que procederá ao tratamento das queixas (nomeadamente qualquer estabelecimento competente na União que possa responder a questões e queixas) e sobre os mecanismos independentes de tratamento das queixas.

(44) Após a receção de uma queixa individual, independentemente de ser apresentada diretamente pelo interessado ou através do *Department of Commerce* na sequência de um reenvio por uma APD, a organização deve fornecer uma resposta ao titular de dados da UE num prazo de 45 dias. Esta resposta deve incluir uma apreciação do mérito da queixa e informações sobre a maneira como a organização resolverá o problema. Do mesmo modo, as organizações devem responder rapidamente às questões e a outros pedidos de informação relativos à sua adesão aos princípios que lhes são dirigidos pelo *Department of Commerce* ou por uma APD ([39]) (quando a organização se comprometeu a cooperar com a APD). As organizações devem conservar arquivos sobre a execução das suas políticas de privacidade e disponibilizá-los, mediante pedido, a uma instância de recurso independente ou à FTC (ou a outra autoridade dos EUA com competência para investigar práticas desleais e enganosas), no quadro de uma investigação ou de uma queixa por não conformidade.

(45) Em segundo lugar, os titulares de dados podem também apresentar uma queixa diretamente junto de um *organismo independente de resolução de litígios* (quer nos Estados Unidos ou na União) designado pela organização para investigar e resolver queixas individuais (a menos que sejam evidentemente infundadas ou abusivas) e para proporcionar uma via de recurso adequada a título gratuito para o titular dos dados. As reparações e sanções aplicadas por tal organismo devem ser suficientemente rigorosas para garantir a conformidade das organizações com os princípios e devem prever uma inversão ou correção, por parte da organização, dos efeitos do incumprimento e, em função das circunstâncias, a cessação da continuação do tratamento dos dados pessoais em causa e/ou a sua eliminação, bem como a publicação no que se refere a casos de incumprimento. Os organismos independentes para a resolução de litígios designados por uma organização serão obrigados a incluir nos seus sítios *web* públicos informações pertinentes sobre o Escudo de Proteção da Privacidade UE-EUA e os serviços que prestam neste âmbito. Todos os anos, devem publicar um relatório anual com estatísticas agregadas relativas a estes serviços ([40]).

([39]) Trata-se da autoridade responsável pelo tratamento designada pelo painel das APD previsto no princípio suplementar sobre «O papel das autoridades responsáveis pela proteção dos dados» Secção III.5 do anexo II).

([40]) O relatório anual deve incluir o seguinte: 1) o número total de queixas relacionadas com o Escudo de Proteção da Privacidade recebidas durante o ano de referência; 2) os tipos de queixas recebidas; 3) as medidas de qualidade da resolução de litígios, tais como o período necessário para o tratamento da queixa; e 4), os resultados das queixas recebidas, designadamente o número e os tipos de reparações ou sanções aplicadas.

(46) Como parte dos seus procedimentos de análise da conformidade, o *Department of Commerce* verificará se as empresas autocertificadas dos EUA se registaram efetivamente junto dos mecanismos de recurso independentes nos quais alegam estar registadas. Tanto as organizações como os mecanismos de recurso independentes responsáveis devem responder imediatamente às questões e aos pedidos de informações apresentados pelo *Department of Commerce* sobre o Escudo de Proteção da Privacidade.

(47) Nos casos em que a organização não cumpra a decisão de um organismo de autorregulação ou de resolução de litígios, este último deve notificar o incumprimento ao *Department of Commerce* e à FTC (ou a outra autoridade dos EUA com competência para investigar práticas desleais e enganosas), ou a um tribunal competente ([41]). Se uma organização se recusar a cumprir uma decisão definitiva de um organismo de autoregulação, um organismo independente de resolução de conflitos, ou um organismo público competente em matéria de privacidade, ou quando o referido organismo determinar que uma organização não cumpre frequentemente os princípios, tal será considerado como um incumprimento sistemático o que implica que o *Department of Commerce*, após dar à organização que não cumpriu um pré-aviso de 30 dias e uma oportunidade para responder, eliminará a referida organização da lista ([42]). Se, uma vez suprimida da lista, a organização continuar a alegar a sua certificação de participação no Escudo de Proteção da Privacidade, o *Department of Commerce* submeterá a questão à FTC ou outro organismo com funções coercivas ([43]).

(48) Em terceiro lugar, as pessoas também podem apresentar as suas queixas a uma *autoridade nacional responsável pela proteção dos dados*. As organizações são obrigadas a cooperar na investigação e a resolução de uma queixa por uma APD, quer no que diz respeito ao tratamento de dados de recursos humanos recolhidos no contexto de uma relação laboral ou quando a entidade respetiva se tenha submetido voluntariamente à supervisão por parte das APD. Designadamente, as organizações devem responder a questões, respeitar o aconselhamento prestado pela APD, incluindo no que se refere a medidas de reparação ou compensação e a apresentar à APD uma confirmação escrita de que as referidas medidas foram tomadas.

(49) O aconselhamento das APD será veiculado através de um painel informal das APD composto por estas autoridades à escala da União ([44]), que contribuirá para assegurar uma abordagem coerente e harmonizada em relação a uma determinada queixa. A resposta será emitida após ter sido dada a ambas as partes envolvidas a oportunidade de apresentar observações e de fornecer todas as informações sobre as provas que considerem necessárias. O painel fornecerá aconselhamento o mais rapidamente possível, dentro dos limites processuais permitidos, regra geral, nos 60 dias seguintes à receção da queixa. Se uma organização não aplicar o conselho da APD no prazo de 25 dias, sem apresentar uma razão válida para o atraso, o painel comunicará a sua intenção de levar o caso à FTC (ou a outra autoridade de execução competente dos EUA), ou de concluir que o compromisso de cooperação foi seriamente violado. Na primeira alternativa, tal conduzirá a medidas de execução com base na secção 5 da FTC Act (ou lei semelhante). Na segunda alternativa, o painel informará o *Department of Commerce*, que considerará a recusa da organização de cumprir o conselho do painel como um incumprimento persistente conducente à supressão da organização da lista do Escudo de Proteção da Privacidade.

(50) Se a APD à qual a queixa foi apresentada não tomar medidas ou tomar medidas insuficientes para a sua resolução, o queixoso tem a possibilidade de contestar tal (in)ação junto dos tribunais nacionais do respetivo Estado-Membro.

(51) As pessoas também podem apresentar queixas às APD, mesmo quando o painel das APD não tiver sido designado como organismo de resolução de litígios de uma organização. Nestes casos, a APD pode remeter essas queixas quer para o *Department of Commerce* quer para a FTC. Para facilitar e reforçar a cooperação em questões relacionadas com queixas individuais e com o incumprimento por parte das organizações participantes no Escudo de Proteção da Privacidade, o *Department of Commerce* criará um ponto de contacto específico que servirá de ponto de ligação com as APD e assisti-las-á nas investigações sobre o cumprimento dos princípios por parte de uma organização ([45]). Do mesmo modo, a FTC comprometeu-se a criar um ponto de contacto específico ([46]) e a prestar assistência às APD nas suas investigações nos termos do *U.S. Safe* web *Act* (lei relativa à segurança da *web*) ([47]).

([41]) Ver a secção III.11.e. do anexo II.
([42]) Ver a secção III.11.g. do anexo II, em especial os pontos ii) e iii).
([43]) Ver anexo I, secção sobre «Procura e Resolução de falsas declarações de participação».
([44]) O regulamento interno do painel informal da APD deve ser estabelecido pelas APD com base na sua competência para organizar o seu trabalho e cooperar entre si.
([45]) Ver o anexo I, secções sobre «Reforço da cooperação com as APD» e «Facilitar a resolução de queixas por incumprimento», bem como a secção II.7.e. do anexo II.
([46]) Ver anexo IV, p.6.
([47]) *Ibid*.

(52) Em quarto lugar, o *Department of Commerce* comprometeu-se a receber, verificar e envidar os melhores esforços para resolver queixas sobre o incumprimento dos princípios por parte de uma organização. Para esse efeito, o *Department of Commerce* prevê procedimentos especiais para que as APD reenviam queixas a um ponto de contacto dedicado, procedam ao seu rastreio e acompanhem as empresas a fim de facilitar a resolução. Com o intuito de acelerar o tratamento de queixas individuais, o ponto de contacto estabelecerá um contacto direto com a respetiva APD sobre questões de conformidade e, em especial, mantê-la-á atualizada sobre o estado das queixas num prazo máximo de 90 dias após a apresentação da queixa. Tal permite que os titulares de dados apresentem queixas de incumprimento imputadas a empresas autocertificadas dos EUA diretamente à sua APD nacional e que estas sejam transmitidas ao *Department of Commerce* enquanto autoridade dos EUA que administra o Escudo de Proteção da Privacidade dos EUA. O *Department of Commerce* também se comprometeu a apresentar, na análise anual do funcionamento do Escudo de Proteção da Privacidade UE-EUA, um relatório que analisa de forma agregada as queixas recebidas todos os anos ([48]).

(53) Se, com base nas suas verificações sistemáticas, queixas ou quaisquer outras informações, o *Department of Commerce* concluir que uma organização persistiu em não cumprir os princípios de privacidade, suprimirá a referida organização da lista do Escudo de Proteção da Privacidade. A recusa em cumprir uma decisão final de qualquer organização de autorregulação em matéria de proteção da privacidade, organismo independente de resolução de litígios ou entidade pública, incluindo a APD, será considerada um incumprimento persistente.

(54) Em quinto lugar, uma organização participante no Escudo de Proteção da Privacidade deve estar sujeita aos poderes de investigação e de execução das autoridades dos Estados Unidos, em especial a *Federal Trade Commission (FTC)* ([49]), que garantirá de forma eficaz o cumprimento dos princípios. A FTC dará prioridade às queixas de incumprimento dos princípios de privacidade submetidas por organismos independentes de resolução de litígios ou de autorregulação, pelo *Department of Commerce* e pelas APD (por iniciativa própria ou após a receção de queixas) a fim de determinar se a secção 5 da FTC Act (lei relativa à Comissão reguladora do comércio federal) foi violada ([50]). A FTC comprometeu-se a criar um processo de transmissão de queixas normalizado, a designar um ponto de contacto no organismo para a receção de queixas das APD e a proceder ao intercâmbio de informações sobre as mesmas. Além disso, aceitará queixas diretamente de pessoas singulares e procederá a investigações no âmbito do Escudo de Proteção da Privacidade por iniciativa própria, nomeadamente como parte das suas investigações em maior escala sobre questões relacionadas com a privacidade.

(55) A FTC pode assegurar a conformidade através de decisões administrativas («injunções») e controlará sistematicamente a conformidade com estas decisões. Sempre que as organizações não as cumpram, a FTC pode submeter o caso ao tribunal competente a fim de solicitar sanções de caráter civil e outras reparações, designadamente por quaisquer danos provocados pela conduta ilegal. Em alternativa, a FTC pode solicitar diretamente uma injunção temporária ou permanente ou outras reparações junto de um tribunal federal. Cada injunção emitida junto de uma organização participante no Escudo de Proteção da Privacidade conterá disposições de comunicação pela própria organização ([51]), e as organizações serão obrigadas a publicar todas as secções pertinentes relacionadas com o Escudo de Proteção da Privacidade dos relatórios de conformidade ou avaliação apresentados à FTC. Por último, a FTC manterá uma lista em linha das empresas objeto de decisões judiciais ou da FTC em processos relativos ao Escudo de Proteção da Privacidade.

(56) Em sexto lugar, enquanto mecanismo de «último recurso», caso nenhuma das restantes vias de recurso tenha resolvido a queixa de forma satisfatória, o titular de dados da UE pode invocar arbitragem vinculativa pelo *«Comité do Escudo de Proteção da Privacidade»*. As organizações devem informar as pessoas sobre a possibilidade, em certas condições, de invocar a arbitragem vinculativa e são obrigadas a responder quando uma pessoa recorrer a esta opção, notificando a organização em causa ([52]).

([48]) Ver anexo I, secção sobre «Facilitar a resolução de queixas por incumprimento».

([49]) Uma organização participante no Escudo de Proteção da Privacidade tem de declarar publicamente o seu compromisso em cumprir os princípios, divulgar publicamente as suas políticas de proteção da privacidade em conformidade com estes princípios e aplicá-los na íntegra. O não cumprimento tem força executória nos termos da secção 5 da *FTC Act*, que proíbe atos desleais e enganosos no comércio ou que afetem o comércio.

([50]) Segundo informações da FTC, não tem competências para realizar inspeções no local no âmbito da proteção da privacidade. Contudo, tem o poder de obrigar as organizações a apresentar documentos e declarações de testemunhas (ver secção 20 da FTC Act), podendo utilizar o sistema judicial para fazer cumprir essas decisões em caso de incumprimento.

([51]) As decisões judiciais ou da FTC podem exigir que as empresas implementem programas de proteção da privacidade e elaborem regularmente relatórios de conformidade ou avaliações independentes por terceiros desses programas acessíveis à FTC.

([52]) Ver a secção II.1.xi e III.7.c. do anexo II.

(57) Este comité arbitral será constituído por um grupo de, pelo menos, 20 árbitros nomeados pelo *Department of Commerce* e a Comissão com base na sua independência, integridade, bem como experiência na legislação dos EUA em matéria de proteção da privacidade e na legislação da União em matéria de proteção dos dados. Para cada litígio individual, as partes selecionarão a partir deste grupo um conjunto de um ou três ([53]) árbitros. Os procedimentos serão regidos por regras de arbitragem normalizadas a acordar entre o *Department of Commerce* e a Comissão. Estas regras completarão o quadro já concluído que contém vários elementos que reforçam a acessibilidade deste mecanismo para os titulares de dados da UE: i) na preparação de uma queixa a apresentar junto do comité, o titular de dados pode ser assistido pela sua APD nacional; ii) embora a arbitragem ocorra nos Estados Unidos, os titulares de dados da UE podem optar por participar através de videoconferência ou conferência telefónica, que será fornecida sem custos para o titular dos dados; iii) embora a arbitragem ocorra em inglês, mediante um pedido fundamentado, regra geral ([54]), será fornecida interpretação na audição arbitral, bem como tradução, sem custos para o titular dos dados, iv) finalmente, embora cada parte tenha de suportar os honorários do próprio advogado, se for representada por um advogado perante o comité, o *Department of Commerce* criará um fundo alimentado por contribuições anuais das organizações participantes no Escudo de Proteção da Privacidade, que devem cobrir os custos elegíveis do procedimento arbitral, até aos montantes máximos, a determinar pelas autoridades dos EUA em consulta com a Comissão.

(58) O Comité do Escudo de Proteção da Privacidade terá competência para aplicar as «medidas equitativas, específicas do titular dos dados e não monetárias» ([55]) necessárias para corrigir o incumprimento dos princípios. Embora o comité tome em consideração outras reparações já obtidas por outros mecanismos do Escudo de Proteção da Privacidade no estabelecimento da sua decisão, as pessoas podem recorrer a arbitragem se considerarem que estas outras reparações são insuficientes. Tal permitirá que os titulares de dados da UE invoquem arbitragem em todos os casos nos quais a ação ou inação das autoridades competentes dos EUA (por exemplo, da FTC) não tenha resolvido as suas queixas de forma satisfatória. Não é possível invocar arbitragem se uma APD tiver autoridade jurídica para resolver a queixa em questão no que se refere à empresa autocertificada dos EUA, nomeadamente nos casos em que a organização é obrigada a cooperar e a respeitar o aconselhamento das APD no respeitante ao tratamento de dados relativos a recursos humanos ou se tiver comprometido voluntariamente a tal. As pessoas podem executar a decisão de arbitragem nos tribunais dos EUA ao abrigo da *Federal Arbitration Act* (lei relativa à arbitragem federal), garantindo assim um recurso jurídico em caso de incumprimento por parte da empresa.

(59) Em sétimo lugar, quando uma organização não cumpra o seu compromisso de respeitar os princípios e a política pública em matéria de proteção da vida privada, podem encontrar-se disponíveis vias de recurso judicial adicionais ao abrigo da legislação dos Estados dos EUA que proporcionem reparações nos termos do direito civil e nos processos de declarações fraudulentas, atos desleais ou enganosos, ou incumprimento de contrato.

(60) Além disso, quando uma APD, depois da receção de uma queixa apresentada por um titular de dados da UE, considere que a transferência dos dados pessoais de uma pessoa para uma organização nos Estados Unidos é realizada em violação da legislação da UE em matéria de proteção de dados, nomeadamente quando o exportador dos dados da UE tem razões para crer que a organização não respeita os princípios, pode igualmente exercer as suas competências face ao exportador de dados e, se necessário, ordenar a suspensão da transferência dos dados.

(61) Tendo em conta as informações constantes da presente secção, a Comissão considera que os princípios emitidos pelo *Department of Commerce* dos EUA, asseguram, enquanto tal, um nível de proteção dos dados pessoais que é essencialmente equivalente ao assegurado pelos princípios substantivos de base estabelecidos na Diretiva 95/46/CE.

(62) Além disso, as obrigações de transparência bem como a análise da administração do cumprimento do Escudo de Proteção da Privacidade pelo *Department of Commerce* garantem a aplicação eficaz dos princípios.

(63) Além disso, a Comissão considera que, como um todo, os mecanismos de recurso e aplicação previstos pelo Escudo de Proteção da Privacidade permitem, na prática, a identificação e sanção das infrações aos princípios por parte das organizações aderentes ao Escudo de Proteção da Privacidade e oferecem vias de recurso ao titular de dados que lhe dão acesso aos seus dados pessoais e permitem a retificação ou eliminação de tais dados.

([53]) O número de árbitros no comité deverá ser acordado entre as partes.

([54]) Todavia, o comité pode concluir que, tomando em consideração as circunstâncias da arbitragem específica, a cobertura conduziria a custos injustificados ou desproporcionados.

([55]) As pessoas não podem solicitar uma indemnização na arbitragem, mas, por sua vez, a invocação de arbitragem não excluirá a opção de solicitar uma indemnização nos tribunais comuns dos EUA.

3. ACESSO E UTILIZAÇÃO DE DADOS PESSOAIS, TRANSFERIDOS AO ABRIGO DO ESCUDO DE PROTEÇÃO DA PRIVACIDADE UE-EUA, PELAS AUTORIDADES PÚBLICAS DOS EUA

(64) Tal como decorre do anexo II, secção I, ponto 5, a adesão aos princípios limita-se ao necessário para observar os requisitos de segurança nacional, interesse público ou aplicação da lei.

(65) A Comissão avaliou as limitações e garantias disponíveis na legislação dos EUA no que se refere ao acesso e à utilização de dados pessoais, transferidos ao abrigo do Escudo de Proteção da Privacidade UE-EUA, pelas autoridades públicas dos EUA para efeitos de segurança nacional, de exercício de funções coercivas e outros fins de interesse público. Além disso, o governo dos EUA, através do seu *Office of the Director of National Intelligence* (ODNI) ([56]), apresentou à Comissão declarações e compromissos pormenorizadas que constam do anexo VI da presente decisão. Por carta assinada pelo *Secretary of State* e que figura na anexo III da presente decisão, o governo dos EUA também se comprometeu a criar um novo mecanismo de supervisão da ingerência da segurança nacional, o Mediador para o Escudo de Proteção da Privacidade, que é independente do setor das informações. Por último, uma declaração do *Department of Justice* (equivalente ao Ministério da Justiça) dos EUA, constante do anexo VII da presente decisão, descreve as limitações e garantias aplicáveis ao acesso e à utilização de dados pelas autoridades públicas para efeitos de aplicação da lei e outros fins de interesse público. Para aumentar a transparência e refletir a natureza jurídica destes compromissos, cada um dos documentos enumerados e que figuram em anexo à presente decisão será publicado no Registo Federal dos EUA.

(66) As conclusões da Comissão sobre as limitações ao acesso e à utilização de dados pessoais, transferidos da União Europeia para os Estados Unidos, pelas autoridades públicas dos EUA e a existência de proteção jurídica efetiva são explicadas em maior pormenor abaixo.

3.1. *Acesso e utilização pelas autoridades públicas dos EUA para efeitos de segurança nacional*

(67) A análise da Comissão demonstra que a legislação dos EUA contém um certo número de limitações ao acesso e utilização de dados pessoais transferidos ao abrigo do Escudo de Proteção da Privacidade UE-EUA para efeitos de segurança nacional, bem como mecanismos de supervisão e reparação que proporcionam garantias suficientes para a proteção eficaz dos dados contra a ingerência ilegal e o risco de abuso ([57]). Desde 2013, quando a Comissão emitiu as suas duas comunicações (ver considerando 7), este enquadramento jurídico foi significativamente reforçado, tal como descrito seguidamente.

3.1.1. Limitações

(68) Nos termos da Constituição dos EUA, o Presidente, na qualidade de Comandante Supremo e Chefe do Executivo, é responsável por garantir a segurança nacional e, no que diz respeito às informações externas, é responsável pelos negócios estrangeiros dos EUA ([58]). Embora o Congresso tenha competência para impor limitações, e o tenha feito em vários aspetos, o Presidente dentro destes limites pode administrar as atividades do setor das informações dos EUA, nomeadamente através de decretos executivos ou diretivas presidenciais. Tal é igualmente aplicável aos domínios nos quais não existem orientações do Congresso. Atualmente, os dois instrumentos jurídicos centrais a este respeito são o Decreto Executivo n.º 12333 («E.O. 12333») ([59]) e a *Presidential Policy Directive* 28.

([56]) O *Director of National Intelligence* (DNI) funciona como chefe do setor das informações e como principal conselheiro do Presidente e do *National Security Council* (Conselho Nacional de Segurança). Ver a *Intelligence Reform and Terrorism Prevention Act* (lei relativa à reforma do sistema de informação e à prevenção do terrorismo) de 2004, Pub. L. 108-458 de 17.12.2004. Entre outros, o ODNI deve determinar os requisitos para, bem como gerir e administrar, a atribuição de missões, a recolha, a análise, a produção e a divulgação de informações nacionais pelo setor das informações, nomeadamente através do desenvolvimento de diretrizes sobre a forma como os dados ou informações são acedidos, utilizados e partilhados. Ver secção 1.3 (a), (b) do E.O. n.º 12333.

([57]) Ver *Schrems*, n.º 91.

([58]) Constituição dos EUA, artigo II. Ver também a introdução à PPD-28.

([59]) E.O. 12333: *United States Intelligence Activities*, Federal Register Vol. 40, n.º 235 (8 de dezembro de 1981). Na medida em que o decreto executivo se encontre acessível ao público, este define os objetivos, as orientações, os deveres e as responsabilidades da procura de informações dos EUA (incluindo o papel dos vários elementos do setor das informações) e estabelece os parâmetros gerais de conduta das atividades dos serviços de informações (em especial a necessidade de promulgar regras processuais específicas). Segundo a secção 3.2. do Decreto Executivo n.º 12333, o Presidente, apoiado pelo *National Security Council*, e o DNI devem emitir as diretivas, os procedimentos e orientações adequados necessários para dar cumprimento ao decreto.

(69) A *Presidential Policy Directive* 28 («PPD-28»), emitida em 17 de janeiro de 2014, impõe várias limitações às operações de «informação de origem eletromagnética» ([60]). Esta PPD é vinculativa para os serviços de informações norte-americanos ([61]) e permanece em vigor após a alteração da administração dos EUA ([62]). A PPD-28 é de especial importância para os cidadãos de países terceiros, nomeadamente para os titulares de dados da UE. Entre outras coisas, estabelece que:

a) a recolha de informação de origem eletromagnética deve basear-se numa lei ou autorização presidencial, e deve ser efetuada de acordo com a Constituição dos EUA (em especial a Quarta Emenda) e a legislação dos EUA;

b) todas as pessoas devem ser tratadas com dignidade e respeito, independentemente da sua nacionalidade ou local de residência;

c) todas as pessoas têm interesses legítimos à privacidade no tratamento das suas informações pessoais;

d) a privacidade e as liberdades cívicas devem ser considerações tomadas em conta no planeamento das atividades de informação de origem eletromagnética dos EUA;

e) As atividades de informação de origem eletromagnética devem, portanto, incluir garantias adequadas para as informações pessoais de todas as pessoas, independentemente da sua nacionalidade ou local de residência.

(70) A PPD-28 estabelece que as informações de origem eletromagnética podem ser recolhidas exclusivamente nos casos em que exista um objetivo de espionagem externa ou de contraespionagem ou para apoiar missões nacionais e departamentais e não para qualquer outro fim (por exemplo, para proporcionar uma vantagem concorrencial às empresas dos EUA). Relativamente a este aspeto, o ODNI explica que os serviços de informações «devem exigir que, sempre que possível, a recolha incida em objetivos ou temas de informação externa específicos através da utilização de discriminantes (por exemplo, mecanismos específicos, termos de seleção e identificadores)» ([63]). Além disso, as declarações fornecem garantias de que as decisões sobre a recolha de informações não são deixadas à discrição dos agentes dos serviços de informações, estando sujeitas às políticas e aos procedimentos que os vários serviços do setor das informações dos EUA são obrigados a adotar para aplicar a PPD-28 ([64]). Por conseguinte, a investigação e determinação de seletores adequados ocorre no âmbito do «*National Intelligence Priorities Framework*» (NIPF) (quadro das prioridades dos serviços de informações nacionais — NIPF) que assegura que as prioridades em termos de informações são definidas por decisores políticos de alto nível e regularmente reexaminadas para que continuem a responder às ameaças reais à segurança nacional, tendo em em consideração os possíveis riscos relacionados para a privacidade ([65]). Com base no que precede, o pessoal dos serviços de informações investiga e identifica termos de seleção específicos que devem recolher informações externas que dão resposta às prioridades ([66]). Os termos de seleção ou «seletores» devem ser regularmente reexaminados para determinar se ainda proporcionam informações valiosas em conformidade com as prioridades ([67]).

([60]) Segundo o O.E. 12333, o diretor da *National Security Agency* (Agência Nacional de Segurança —NSA) é o administrador funcional da informação de origem eletromagnética e deve gerir uma organização unificada em matéria de atividades de informação de origem eletromagnética.

([61]) Para a definição do termo «setor das informações» ver a secção 3.5 (h) do Decreto Executivo n.º 12333 com o n.º 1 da PPD-28.

([62]) Ver Memorando do *Office of Legal Counsel, Department of Justice* (DOJ), ao Presidente Clinton, 29 de janeiro de 2000. De acordo com este parecer jurídico, as diretivas presidenciais têm o mesmo «efeito jurídico substantivo que um decreto executivo».

([63]) Declarações do ODNI (anexo VI), p. 3.

([64]) Ver secção 4(b),(c) da PPD-28. De acordo com as informações públicas, a reapreciação de 2015 confirmou a existência de seis objetivos. Ver ODNI, *Signals Intelligence Reform*, Relatório dos progressos realizados de 2016.

([65]) Declarações do ODNI (anexo VI), p. 6 (com referência à *Intelligence Community Directive* 204). Ver também secção 3 da PPD-28.

([66]) Declarações do ODNI (anexo VI), p. 6. Ver por exemplo, *NSA Civil Liberties and Privacy Office* (NSA CLPO), *NSA's Civil Liberties and Privacy Protections for Targeted SIGINT Activities under Executive Order* 12333, 7 de outubro de 2014. Ver também o relatório de situação do ODNI relativo a 2014. No que se refere aos pedidos de acesso ao abrigo da secção 702 da FISA, as questões são regidas pelos procedimentos de minimização aprovados pelo FISC. Ver NSA CLPO, *NSA's Implementation of Foreign Intelligence Surveillance Act Section* 702, 16 de abril de 2014.

([67]) Ver *Signals Intelligence Reform, 2015 Anniversary Report*. Ver também declarações do ODNI (anexo VI), p. 6, 8-9, 11.

(71) Além disso, os requisitos estabelecidos na PPD-28 segundo os quais a recolha de informações deve ser sempre ([68]) «a mais adaptada possível», e o setor das informações deve dar prioridade à disponibilidade de outras informações e alternativas adequadas e viáveis ([69]) refletem uma regra geral do estabelecimento de prioridades de uma recolha seletiva em detrimento de uma recolha em larga escala. Segundo a declaração da ODNI, garantem, em especial, que a recolha em larga escala não é «em massa» nem «indiscriminada», e que a exceção não substitui a regra ([70]).

(72) Embora a PPD-28 explique que os elementos do setor das informações devem, por vezes recolher informação de origem eletromagnética em larga escala em determinadas circunstâncias, por exemplo, para identificar e avaliar ameaças novas ou emergentes, estabelece que esses elementos devem dar prioridade a alternativas que permitam a recolha de informação seletiva de origem eletromagnética ([71]). Daqui resulta que a recolha em larga escala só será autorizada quando a recolha seletiva através da utilização de discriminantes — isto é, identificadores associados a um objetivo específico (como o correio eletrónico ou o número do telefone do objetivo) — não possa realizar-se por motivos técnicos ou operacionais ([72]). O que precede é aplicável à forma de recolha da informação de origem eletromagnética e ao conteúdo que é efetivamente recolhido ([72]).

(73) Segundo as declarações da ODNI, mesmo quando os serviços de informações não puderem utilizar identificadores específicos para especificar a recolha, aqueles procurarão reduzir a recolha «tanto quanto possível». Para garantir isto, «aplicarão filtros e outras ferramentas técnicas para centrar a recolha nas instalações suscetíveis de conter comunicações com valor para as informações externas» (dando assim resposta a requisitos dos responsáveis políticos dos Estados Unidos no que diz respeito ao procedimento descrito no ponto 70). Como consequência deste facto, a recolha em larga escala centrar-se-á, pelo menos, de duas maneiras: em primeiro lugar, dirá sempre respeito a objetivos específicos de informações externas (por exemplo, adquirir informação de origem eletromagnética sobre as atividades de um grupo terrorista que opera numa determinada região) e centrar a recolha em comunicações que possuem esse nexo. Segundo a garantia dada pelo ODNI, tal reflete-se no facto de as atividades de informação de origem eletromagnética dos Estados Unidos se referirem apenas a uma fração das comunicações através da Internet ([73]). Em segundo lugar, as declarações do ODNI explicam que os filtros e outros instrumentos técnicos utilizados serão concebidos para centrará a recolha «da forma mais exata possível», a fim de garantir que a quantidade de «informação não pertinente» recolhida seja mínima.

(74) Por último, mesmo nos casos em que os Estados Unidos consideram necessário efetuar a recolha em grande escala de informação de origem eletromagnética, nas condições estabelecidas nos considerandos 70-73, a PPD-28 limita a utilização desta informação a uma lista específica de seis objetivos de segurança nacional com vista a proteger a privacidade e as liberdades cívicas de todas as pessoas, independentemente da sua nacionalidade ou local de residência ([74]). Estes objetivos admissíveis englobam medidas de deteção e combate a ameaças

([68]) Ver declarações do ODNI (anexo VI), p. 3.

([69]) Importa ainda salientar que, de acordo com a secção 2.4 do Decreto Executivo n.º 12333, os serviços de informações «devem utilizar os meios de recolha menos invasivos possíveis nos Estados Unidos». No que se refere às limitações de substituir todas as recolhas em larga escala por recolhas seletivas, ver os resultados de uma avaliação do *National Research Council*, tal como informou a Agência dos Direitos Fundamentais da União Europeia, Vigilância por parte de serviços de informação: direitos fundamentais, salvaguardas e recursos na UE (2015), p. 18.

([70]) Declarações do ODNI (anexo VI), p. 4.

([71]) Ver também a secção 5(d) da PPD-28, que estabelece que o *Director of National Intelligence* (Diretor dos Serviços Nacionais de Informações), em coordenação com os chefes dos elementos competentes do setor das informações e o *Office of Science and Technology Policy* (Gabinete da Política Científica e Tecnológica) devem apresentar ao Presidente um «relatório de avaliação da viabilidade da criação de um software que permita ao setor das informações a recolha mais fácil de informações seletivas em vez de uma recolha em larga escala». De acordo com as informações públicas, este relatório concluiu que «não existe um software alternativo que substitua na íntegra a recolha em larga escala na deteção de algumas ameaças para a segurança nacional». Ver *Signals Intelligence Reform, 2015 Anniversary Report*.

([72]) Ver nota 68.

([73]) Declarações do ODNI (anexo VI). Isto aborda especificamente a preocupação expressa pelas autoridades nacionais de proteção de dados no seu parecer sobre o projeto de decisão de adequação. Ver o Parecer 1/2016 do grupo de trabalho do artigo 29.º sobre a proteção de dados, sobre o projeto de decisão de adequação sobre o Escudo de Proteção da Privacidade UE-EUA (adotado em 13 de abril de 2016), p. 38, n.º 47.

([74]) Ver secção 2 da PPD-28.

decorrentes de espionagem, terrorismo, armas de destruição maciça, ameaças à cibersegurança, para as forças armadas ou o pessoal militar, bem como ameaças criminosas transnacionais relacionadas com os restantes cinco objetivos e serão reexaminados, pelo menos, anualmente. De acordo com as declarações do governo dos EUA, os elementos do setor das informações reforçaram as suas normas e práticas analíticas para a consulta de informação de origem eletromagnética não avaliada a fim de cumprir estes requisitos; a utilização de consultas seletivas «assegura que apenas os elementos que se consideram deter um potencial valor informativo são apresentados aos analistas para efeitos de análise». ([75])

(75) Estas limitações são de especial relevância para os dados pessoais transferidos ao abrigo do Escudo de Proteção da Privacidade, nomeadamente se a recolha de dados pessoais ocorrer fora dos Estados Unidos da América, designadamente durante o seu trânsito nos cabos transatlânticos da União para os Estados Unidos. Tal como confirmado pelas autoridades dos EUA nas declarações do ODNI, as limitações e garantias aí estabelecidas — designadamente as da PPD-28 — são aplicáveis a tal recolha ([76]).

(76) Embora não enunciados nesses termos jurídicos, estes princípios refletem a essência dos princípios de necessidade e proporcionalidade. É evidentemente atribuída prioridade à recolha seletiva, ao passo que a recolha em larga escala é limitada a situações (excecionais) nas quais a recolha seletiva não é possível por motivos técnicos ou operacionais. Mesmo nos casos em que não seja possível evitar a *recolha em larga escala*, a «utilização» posterior de tais dados através do acesso é *estritamente limitada* a objetivos de segurança nacional específicos e legítimos ([77]).

(77) Enquanto diretiva emitida pelo Presidente na qualidade de Chefe do Executivo, estes requisitos são vinculativos para todo o setor das informações e foram posteriormente aplicados através das normas e procedimentos dos serviços que transpõem os princípios gerais em orientações específicas para as operações quotidianas. Além disso, embora o Congresso em si não esteja vinculado pela PPD-28, também tomou medidas para garantir que a recolha e o acesso a dados pessoais nos Estados Unidos são seletivos e não executados «de forma generalizada».

(78) Decorre das informações disponíveis, nomeadamente das declarações recebidas do governo dos EUA, que após a transferência dos dados para organizações localizadas nos Estados Unidos e autocertificadas ao abrigo do Escudo de Proteção da Privacidade UE-EUA, os serviços de informações dos EUA só podem ([78]) solicitar dados pessoais nos casos em que o seu pedido respeite a *Foreign Intelligence Surveillance Act* (lei relativa à vigilância dos serviços de informações externas— FISA) ou seja efetuado pelo *Federal Bureau of Investigation* (FBI) (Gabinete Federal de Investigação) com base numa denominada *National Security Letter* (carta de segurança nacional — NSL) ([79]). Existem várias bases jurídicas ao abrigo da FISA que podem ser utilizadas para recolher (e subsequentemente tratar) os dados pessoais de titulares de dados da UE transferidos no âmbito do Escudo de Proteção da

([75]) Declarações do ODNI (anexo VI), p. 4. Ver também *Intelligence Community Directive 203*.

([76]) Declarações do ODNI (anexo VI), p. 2. De igual modo, as limitações estipuladas no Decreto Executivo n.º 12333 (por exemplo, a necessidade de a informação recolhida dar resposta às prioridades em termos de informações estabelecidas pelo Presidente) são aplicáveis.

([77]) Ver *Schrems*, n.º 93.

([78]) Além disso, a recolha de dados pelo FBI também se pode basear em autorizações das autoridades que exercem funções coercivas (ver secção 3.2 da presente decisão).

([79]) Para explicações adicionais sobre a utilização de NSL ver as declarações do ODNI (anexo VI) p. 13-14 com n.º 38. Tal como aí indicado, o FBI pode recorrer a NSL apenas para solicitar informações sem conteúdo relevantes para uma investigação de segurança nacional autorizada para efeitos de proteção contra o terrorismo internacional ou atividades clandestinas dos serviços de informações. No que diz respeito às transferências de dados ao abrigo do Escudo de Privacidade UE-EUA, a autorização jurídica mais relevante parecer ser a *Electronic Communications Privacy Act* (lei relativa à proteção das comunicações eletrónicas privadas) (18 U.S.C. § 2709), que exige que qualquer pedido de informações sobre assinantes ou registos transnacionais utilize um «termo que identifique especificamente uma pessoa, entidade, número de telefone ou conta».

Privacidade UE-EUA. Para além da secção 104 da FISA ([80]) que abrange vigilância eletrónica individualizada tradicional e da secção 402 da FISA ([81]) e da instalação de dispositivos de registo de chamadas telefónicas e comunicações eletrónicas, os dois instrumentos centrais são a secção 501 da FISA (antiga secção 215 da *U.S. PATRIOT ACT*) e a secção 702 da FISA ([82]).

(79) A este respeito, a *USA FREEDOM Act*, adotada em 2 de junho de 2015, proíbe a recolha em larga escala de registos com base na secção 402 da FISA (autoridade em matéria de dispositivos de registo de chamadas telefónicas e comunicações eletrónicas), na secção 501 da FISA (antiga secção 215 da Patriot Act) ([83]) e através da utilização de NSL e, em vez disso, exige a utilização de «termos de seleção» específicos ([84]).

(80) Embora a FISA contenha autorizações jurídicas adicionais para a realização de atividades dos serviços de informações nacionais, incluindo informação de origem eletromagnética, a avaliação da Comissão demonstrou que, no que diz respeito aos dados pessoais a transferir ao abrigo do Escudo de Proteção da Privacidade UE-EUA, estas autoridades restringem igualmente a ingerência por parte das autoridades públicas à recolha e ao acesso seletivos.

(81) Tal é evidente no que se refere à vigilância eletrónica individualizada tradicional nos termos da secção 104 da FISA ([85]). Relativamente à secção 702 da FISA, que constitui a base de dois programas de informações importante geridos pelos serviços de informações dos EUA (PRISM, UPSTREAM), as investigações são realizadas de forma seletiva através da utilização de seletores individuais que identificam meios de comunicação específicos, tais como o endereço eletrónico ou o número de telefone da pessoa visada, mas não palavras-chave nem mesmo os nomes das pessoas em causa ([86]). Portanto, tal como referido pela *Privacy and Civil Liberties Oversight Board* (comissão de

([80]) 50 U.S.C. § 1804. Não obstante o facto de esta autoridade jurídica exigir uma «declaração dos factos e circunstâncias subjacentes ao pedido do requerente para justificar a sua convicção de que a) o alvo da vigilância eletrónica é uma potência estrangeira ou um agente de uma potência estrangeira», este último pode incluir cidadãos de países terceiros envolvidos em terrorismo internacional ou na proliferação internacional de armas de destruição maciça (incluindo atos preparatórios) [50 U.S.C. § 1801 (b)(1)]. Contudo, existe apenas uma ligação teórica aos dados pessoais transferidos ao abrigo do Escudo de Proteção da Privacidade UE-EUA, uma vez que a declaração dos factos também deve justificar a convicção de que «cada um dos locais ou meios de comunicação que são alvos da vigilância eletrónica estão a ser utilizados, ou serão em breve utilizados, por uma potência estrangeira ou um agente de uma potência estrangeira». De qualquer modo, a utilização desta autoridade exige a apresentação de um pedido ao FISC que avaliará, entre outras questões, se, com base nos factos apresentados, existe uma causa provável de que tal se verifique efetivamente.

([81]) 50 U.S.C. § 1842 com § 1841(2) e secção 3127 do título 18. Esta autoridade não diz respeito ao conteúdo das comunicações, visando, em vez disso, as informações sobre o cliente ou assinante que utiliza um serviço (tais como nome, endereço, número de cliente, duração/ /tipo de serviço recebido, fonte/mecanismo de pagamento). O que precede exige o pedido de uma decisão emitida pelo FISC (ou por um magistrado dos EUA) e a utilização de um termo de seleção específico na aceção de § 1841(4), isto é, um termo que identifique especificamente, por exemplo, uma pessoa ou conta e seja utilizado para limitar, tanto quanto razoavelmente possível, o âmbito da informação procurada.

([82]) Embora a secção 501 da FISA (antiga secção 215 da *U.S. PATRIOT ACT*) autorize o FBI a solicitar uma decisão judicial destinada à produção de «coisas tangíveis» (nomeadamente metadados telefónicos, mas também documentação relativa à atividade empresarial) para efeitos de informações externas, a secção 702 da FISA permite que os elementos do setor das informações dos EUA solicitem o acesso a informações, nomeadamente ao conteúdo de comunicações na Internet, proveniente dos Estados Unidos, mas que visam determinados cidadãos de países terceiros fora dos Estados Unidos.

([83]) Com base nesta disposição, o FBI pode solicitar «coisas tangíveis» (por exemplo, registos e documentação) com base numa demonstração ao *Foreign Intelligence Surveillance Court* (tribunal encarregado de supervisionar os pedidos e mandatos em matéria de vigilância — FISC) de que existem motivos razoáveis para considerar que são relevantes para uma investigação específica do FBI. Na realização da sua investigação, o FBI deve utilizar termos de seleção aprovados pelo FISC relativamente aos quais exista uma «suspeita razoável e articulável» de que tal termo se encontra associado a uma ou mais potências estrangeiras ou aos seus agentes envolvidos em terrorismo internacional ou atividades de preparação do mesmo. Ver PCLOB, Sec. 215 Report, p. 59; *NSA CLPO, Transparency Report: The USA Freedom Act Business Records FISA Implementation*, 15 de janeiro de 2016, p. 4-6.

([84]) Declarações do ODNI (anexo VI), p. 13 (n.º 38).

([85]) Ver nota de rodapé 81.

([86]) PCLOB, Sec. 702 *Report*, p. 32-33 com referências adicionais. De acordo com o seu serviço de proteção da vida privada, a NSA deve verificar se existe uma relação entre o alvo e o seletor, deve documentar as informações no estrangeiro que prevê obter, estas informações devem ser revistas e aprovadas por dois analistas principais da NSA e o processo global será rastreado para subsequentes verificações de conformidade pelo ODNI e o Department of Justice. Ver *NSA CLPO, NSA's Implementation of Foreign Intelligence Act Section 702*, 16 de abril de 2014.

controlo da privacidade e das liberdades cívicas — PCLOB), a vigilância da secção 702 «consiste exclusivamente em visar cidadãos [de países terceiros] específicos sobre os quais foi feita uma determinação individualizada» ([87]). Devido a uma cláusula de «caducidade», será necessário rever a secção 702 da FISA em 2017, data em que a Comissão terá de reexaminar as garantias à disposição dos titulares de dados da UE.

(82) Além disso, nas suas declarações, o governo dos EUA apresentou garantias explícitas à Comissão Europeia de que o setor das informações dos EUA «não procede à vigilância indiscriminada de ninguém, nomeadamente de cidadãos europeus comuns» ([88]). No que diz respeito aos dados pessoais recolhidos nos EUA, esta declaração é apoiada por dados empíricos que demonstram que os *pedidos de acesso* através de NSL e nos termos da FISA, tanto a nível individual como em conjunto, dizem respeito a um número relativamente reduzido de alvos quando comparados com o fluxo global de dados na Internet ([89]).

(83) No que se refere ao *acesso* a dados recolhidos e à *segurança dos dados*, a PPD-28 exige que o acesso seja «limitado ao pessoal autorizado com necessidade de conhecer as informações para desempenhar a sua missão» e que as informações pessoais «devem ser tratadas e armazenadas em condições que proporcionem uma proteção adequada e impeçam o acesso de pessoas não autorizadas, em conformidade com as garantias aplicáveis às informações sensíveis». O pessoal dos serviços de informações recebe formação apropriada e adequada sobre os princípios estabelecidos na PPD-28 ([90]).

(84) Por último, no que se refere à *conservação* e posterior *divulgação* de dados pessoais de titulares de dados da UE recolhidos pelos serviços de informações dos EUA, a PPD-28 estabelece que todas as pessoas (incluindo cidadãos de países terceiros) devem ser tratadas com dignidade e respeito, que todas as pessoas têm interesses legítimos de privacidade no tratamento dos seus dados pessoais e que os elementos do setor das informações devem, portanto, criar políticas que proporcionem garantias adequadas para os referidos dados «razoavelmente concebidas para minimizar o [seu] risco de divulgação e preservação» ([91]).

([87]) PLCOB, Sec. 702 Report, p. 111. Ver também declarações do ODNI (anexo VI), p. 9 («a recolha nos termos da secção 702 da [FISA] não é maciça e indiscriminada», incidindo estreitamente sobre a recolha de informações externas de alvos legítimos e individualmente identificados) e p. 13, n.º 36 (com referência a um parecer de 2014 do FISC); NSA CLPO, NSA's *Implementation of Foreign Intelligence Act Section* 702, 16 de abril de 2014. Mesmo no caso do programa UPSTREAM, a NSA só pode solicitar a interceção de comunicações eletrónicas de, para ou sobre seletores atribuídos.

([88]) Declarações do ODNI (anexo VI), p. 18. Ver também a p. 6, segundo a qual os procedimentos aplicáveis «demonstram um compromisso evidente para evitar a recolha arbitrária e indiscriminada de informação de origem eletromagnética e aplicar — a partir dos níveis mais elevados do nosso governo — o princípio da razoabilidade».

([89]) Ver *Statistical Transparency Report Regarding Use of National Security Authorities*, 22 de abril de 2015. No que se refere ao fluxo global de dados na Internet, ver, por exemplo, *Fundamental Rights Agency, Surveillance by Intelligence Services*: Direitos fundamentais, salvaguardas e recursos na UE (2015), p. 15-16. No respeitante ao programa UPSTREAM, segundo um parecer desclassificado do FISC de 2011, mais de 90 % das comunicações eletrónicas obtidas nos termos da secção 702 da FISA são provenientes do programa PRISM, ao passo que menos de 10 % são provenientes do programa UPSTREAM. Ver *FISC, Memorandum Opinion*, 2011 WL 10945618 (FISA Ct., 3.10.2011), n.º 21 (disponível em: http://www.dni.gov/files/documents/0716/October-2011-Bates-Opinion-and%20Order-20140716.pdf).

([90]) Ver secção 4(a)(ii) da PPD-28. Ver também ODNI, *Safeguarding the Personal Information of all People*: A *Status Report on the Development and Implementation of Procedures under Presidential Policy Directive* 28, julho de 2014, p. 5, segundo o qual «as políticas dos elementos do setor das informações devem reforçar as normas e práticas analíticas em vigor de acordo com as quais os analistas devem procurar estruturar as consultas ou outros termos e técnicas de pesquisa a fim de identificar informações relevantes para uma missão válida de informação ou aplicação da lei; centrar as consultas sobre pessoas nas categorias de informações que dão resposta a um requisito de informações ou aplicação da lei; e minimizar a análise de informações pessoais não pertinentes para os requisitos em matéria de informação ou aplicação da lei». Ver, por exemplo, CIA, *Signals Intelligence Activities*, p. 5; FBI, *Presidential Policy Directive 28 Policies and Procedures*, p. 3. De acordo com o relatório de progresso de 2016 sobre a reforma da informação de origem eletromagnética, os elementos do setor das informações (nomeadamente o FBI, a CIA e a NSA) tomaram medidas para aumentar a sensibilização do seu pessoal para os requisitos da PPD-28 através da criação de novas políticas de formação ou da alteração das políticas existentes.

([91]) Segundo as declarações da ODNI, estas restrições são aplicáveis independentemente da questão de saber se as informações foram recolhidas em larga escala ou através de uma recolha seletiva, e da nacionalidade do titular dos dados.

(85) O governo dos EUA explicou que este requisito de razoabilidade significa que os elementos do setor das informações não terão de adotar «todas as medidas teoricamente possíveis», mas terão de «equilibrar os seus esforços para proteger os interesses legítimos em matéria de privacidade e liberdades cívicas com as necessidades práticas das atividades de informação de origem eletromagnética» ([92]). A este respeito, os cidadãos de países terceiros serão tratados do mesmo modo que os cidadãos dos EUA, com base nos procedimentos aprovados pelo *Attorney General* ([93]).

(86) De acordo com estas regras, em geral, a preservação limita-se a um período máximo de cinco anos, a menos que exista uma determinação específica na legislação ou uma determinação expressa efetuada pelo *Director of National Intelligence* após uma avaliação cuidadosa das preocupações em matéria de privacidade — tomando em consideração as opiniões do *Civil Liberties Protection Officer* (agente responsável pela proteção das liberdades cívicas) do ODNI, bem como dos funcionários responsáveis pela proteção da privacidade e das liberdades cívicas — de que a preservação continuada é do interesse da segurança nacional ([94]). A divulgação limita-se aos casos nos quais as informações são relevantes para o objetivo subjacente à recolha e, como tal, dão resposta a um pedido autorizado em matéria de aplicação da lei ou informações externas ([95]).

(87) De acordo com as garantias oferecidas pelo governo dos EUA, as informações pessoais não podem ser divulgadas exclusivamente porque o titular dos dados é um cidadão de um país terceiro e «a informação de origem eletromagnética sobre as atividades quotidianas de um estrangeiro não seria considerada informação externa passível de divulgação ou preservação permanente por força simplesmente desse facto, a menos que dê resposta de outro modo a um pedido autorizado em matéria de informações externas» ([96]).

(88) Tendo em conta tudo o que precede, a Comissão conclui que existem normas em vigor nos Estados Unidos destinadas a limitar qualquer ingerência para efeitos de segurança nacional nos direitos fundamentais das pessoas cujos dados pessoais são transferidos da União para os Estados Unidos ao abrigo do Escudo de Proteção da Privacidade UE-EUA ao estritamente necessário para a consecução do objetivo legítimo em questão.

(89) Tal como o mostrou a análise anterior, o direito americano garante que as medidas de vigilância servirão apenas para a obtenção de informações oriundas do estrangeiro, o que constitui um objetivo estratégico legítimo ([97]), e serão o mais possível adaptadas. Em especial, a recolha em larga escala só será autorizada a título excecional,

([92]) Ver declarações do ODNI (anexo VI).

([93]) Ver secção 4(a)(i) da PPD-28 com a secção 2.3 do Decreto Executivo. n.º 12333.

([94]) Secção 4(a)(i) da PPD-28; Declarações do ODNI (anexo VI), p. 7. Por exemplo, no que diz respeito às informações pessoais recolhidas nos termos da secção 702 da FISA, os procedimentos de minimização da NSA aprovados pelo FISC preveem, regra geral, que os metadados e o conteúdo não avaliado do programa PRISM devem ser preservados durante um período máximo de cinco anos, ao passo que os dados do programa UPSTREAM devem ser preservados durante um período máximo de dois anos. A NSA cumpre estes limites de conservação através de um processo automatizado que elimina os dados recolhidos no final do respetivo período de preservação. Ver *NSA Sec. 702 FISA Minimization Procedures, Sec. 7 com Sec. 6(a)(1)*; *NSA CLPO, NSA's Implementation of Foreign Intelligence Surveillance Act Section 702*, 16.4.2014. Igualmente, a preservação nos termos da secção 501 da FISA (antiga secção 215 da *Patriot Act*) limita-se a cinco anos, salvo se os dados pessoais fizerem parte da divulgação devidamente autorizada de informações do estrangeiro ou se o DOJ informar a NSA por escrito de que a documentação está sujeita a uma obrigação de preservação num litígio previsto ou pendente. Ver *NSA, CLPO, Transparency Report: The USA Freedom Act Business Records FISA Implementation*, 15.1.2016.

([95]) Nomeadamente no caso da secção 501 da FISA (antiga secção 215 da Patriot Act), a divulgação de informações pessoais pode ocorrer apenas para efeitos de luta contra o terrorismo ou como prova de um crime; no caso da secção 702 da FISA, apenas se existir um objetivo válido em matéria de aplicação da lei ou informações externas. Ver *NSA, CLPO, NSA's Implementation of Foreign Intelligence Surveillance Act* Secção 702, 16 de abril de 2014; Transparency Report: *The USA Freedom Act Business Records FISA Implementation*, 15 de janeiro de 2016. Ver também *NSA's Civil Liberties and Privacy Protections for Targeted SIGINT Activities under Executive Order 12333*, 7 de outubro de 2014.

([96]) Declarações do ODNI (anexo VI), p. 7 (com referência à *Intelligence Community Directive (ICD) 203*).

([97]) O Tribunal de Justiça especificou que a segurança nacional constitui um objetivo legítimo. Ver *Schrems*, n.º 88. Ver igualmente o acórdão do Tribunal de Justiça proferido no processo *Digital Rights Ireland and Others*, n.ºs 42-44 e 51, no qual o Tribunal de Justiça considerou que a luta contra as formas graves de criminalidade, em especial a criminalidade organizada e o terrorismo pode depender, numa grande medida, da utilização de técnicas modernas de investigação. Além disso, ao contrário do que se passa nas investigações penais, que tradicionalmente dizem respeito à determinação retroativa da responsabilidade e da culpa por comportamentos passados, as atividades dos serviços de informação incidem frequentemente na prevenção de ameaças à segurança nacional antes de ocorrerem danos. Por conseguinte, a referida investigação pode muitas vezes ter de cobrir uma gama mais vasta de eventuais atores («objetivos») e uma área geográfica mais ampla. Ver TEDH, *Weber and Saravia/Alemanha*, Decisão de 29 de junho de 2006, Pedido n.º 54934/00, pontos 105-118 (sobre o denominado «acompanhamento estratégico»).

quando não for viável uma recolha seletiva, sendo acompanhada de salvaguardas adicionais com vista a limitar ao máximo a quantidade de dados recolhidos e o posterior acesso (que deverá ser centrado e autorizado unicamente para fins específicos).

(90) Segundo a apreciação da Comissão, esta prática está conforme à norma fixada pelo Tribunal de Justiça no acórdão *Schrems*, segundo o qual uma legislação que envolva uma ingerência nos direitos fundamentais garantidos pelos artigos 7.º e 8.º da Carta deve impor «um mínimo de exigências» ([98]) e «não se limitar ao mínimo estritamente necessário quando autoriza, de forma generalizada, a conservação de todos os dados pessoais de todas as pessoas cujos dados foram transferidos da União Europeia para os Estados Unidos sem que fosse efetuada qualquer diferenciação, limitação ou exceção, tendo em conta os objetivos prosseguidos e sem que fosse previsto um critério objetivo que permita delimitar o acesso das autoridades públicas aos dados e respetiva utilização ulterior para fins específicos, estritamente restritos e suscetíveis de justificar a ingerência que comportam tanto o acesso como a utilização desses dados». ([99]) Não existirá recolha e armazenamento ilimitados de dados de todas as pessoas sem restrições nem acesso ilimitado. Além disso, as observações apresentadas à Comissão, incluindo a garantia de que as atividades de informação de origem eletromagnética dos EUA dizem respeito apenas a uma pequena parte das comunicações que transitam pela Internet, excluem que se possa aceder «numa base generalizada» ([100]) ao conteúdo das comunicações eletrónicas.

3.1.2. Proteção jurídica efetiva

(91) A Comissão avaliou tanto os mecanismos de supervisão existentes nos Estados Unidos no que se refere a qualquer ingerência pelos serviços de informações dos EUA nos dados pessoais transferidos para os EUA como as vias de recurso individuais acessíveis aos titulares de dados da UE.

Supervisão

(92) O conjunto da comunidade dos serviços de informações dos Estados Unidos está sujeito a diversos mecanismos de controlo e de supervisão que são abrangidos pelas três vertentes do Estado. Trata-se nomeadamente de órgãos internos e externos na vertente executiva, de um certo número de comissões do Congresso, bem como entidades responsáveis pela supervisão judiciária que incide especificamente nas atividades realizadas no quadro da *Foreign Intelligence Surveillance Act*.

(93) Em primeiro lugar, as atividades de informações levadas a cabo pelas autoridades dos EUA são objeto de ampla supervisão por parte do poder executivo.

(94) Segundo a PPD-28, secção 4(a)(iv), as políticas e os procedimentos dos elementos do setor das informações «devem incluir medidas adequadas para facilitar a supervisão da implementação de garantias que protejam as informações pessoais»; estas medidas devem incluir auditorias periódicas ([101]).

([98]) Acórdão *Schrems*, n.º 91, com referências adicionais.
([99]) Acórdão *Schrems*, n.º 93.
([100]) Ver acórdão *Schrems*, n.º 94.
([101]) ODNI, *Safeguarding the Personal Information of all People: A Status Report on the Development and Implementation of Procedures under Presidential Policy Directive 28*, p. 7. Ver, por exemplo, CIA, *Signals Intelligence Activities*, p. 6 (*Compliance*); FBI, *Presidential Policy Directive 28 Policies and Procedures*, Sec. III (A)(4), (B)(4); NSA, PPD-28 *Section 4 Procedures*, 12 de janeiro de 2015, Sec. 8.1, 8.6(c).

(95) Foram instaurados vários níveis de supervisão a este respeito, nomeadamente os agentes responsáveis pela proteção das liberdades cívicas ou da privacidade, os inspetores-gerais, o *Civil Liberties and Privacy Office* (gabinete responsável pela proteção da privacidade e das liberdades cívicas) do ODNI, a PCLOB e a *Intelligence Oversight Board* (comissão de supervisão dos serviços de informações) do Presidente. Estas funções de supervisão são apoiadas pelo pessoal responsável pela conformidade em todos os serviços ([102]).

(96) Tal como explicado pelo governo dos EUA ([103]), *os agentes responsáveis pelas liberdades cívicas ou a privacidade* com responsabilidade de supervisão existem em vários departamentos com responsabilidades em matéria de informações e serviços de informações ([104]). Embora os poderes específicos destes agentes possam variar um pouco em função do estatuto de autorização, normalmente englobam a supervisão dos procedimentos a fim de assegurar que o respetivo departamento/organismo tem em devida consideração a proteção da privacidade e das liberdades cívicas e instaurou procedimentos adequados para a resolução de queixas de pessoas que consideram que a sua privacidade ou liberdades cívicas foram violadas (e, em alguns casos, como o ODNI, podem ter competência para investigar queixas ([105])). O chefe do departamento/organismo, por sua vez, deve assegurar que o agente recebe todas as informações e tem acesso a todos os materiais necessários ao desempenho das suas funções. Os agentes responsáveis pela proteção da privacidade e das liberdades cívicas comunicam periodicamente ao Congresso e à PCLOB, designadamente sobre o número e a natureza das queixas recebidas pelo departamento/ /organismo, bem como um resumo de tais queixas, as análises efetuadas e as questões colocadas e o impacto das atividades levadas a cabo pelo agente ([106]). Segundo a avaliação das autoridades nacionais de proteção dos dados, o controlo interno exercido pelos agentes responsáveis pela proteção da privacidade e das liberdades cívicas pode ser considerado «bastante sólido», mesmo que na sua opinião esses agentes não beneficiem do grau de independência exigido ([107]).

(97) Além disso, cada elemento do setor das informações dispõe do seu próprio *inspetor-geral* que, entre outras funções, é responsável pela supervisão das atividades de informações externas ([108]). Isto inclui, no âmbito do ODNI, um *Office of the Inspector General* (gabinete do inspetor-geral) com competência abrangente sobre todo o setor das informações e autorizado a investigar queixas ou informações respeitantes a alegações de conduta ilegal ou abuso de autoridade relacionadas com o ODNI e/ou programas e atividades do setor das informações ([109]). Os inspetores-gerais são unidades juridicamente independentes ([110]) responsáveis pela realização de auditorias e investigações relacionadas com os programas e operações levados a cabo pelo respetivo serviço para efeitos de segurança nacional, nomeadamente por abuso ou violação da lei ([111]). Estão autorizados a aceder

([102]) Por exemplo, a NSA emprega mais de 300 funcionários responsáveis pela conformidade na *Directorate for Compliance*. Ver declarações do ODNI (anexo VI), p. 7.

([103]) Ver mecanismo de mediação (anexo III), secção 6, alínea b), subalíneas i) a iii).

([104]) Ver 42 U.S.C. § 2000ee-1. Isto inclui, por exemplo, o *Department of State*, o *Department of Justice* (incluindo o FBI), o *Department of Homeland Security*, o *Department of Defense*, a NSA, CIA e o ODNI.

([105]) Segundo o governo dos EUA, se o *Civil Liberties and Privacy Office* do ODNI receber uma queixa, também cooperará com outros elementos do setor das informações no que se refere ao tratamento posterior da queixa no setor das informações. Ver mecanismo de mediação (anexo III), secção 6, alínea b), subalínea ii).

([106]) Ver 42 U.S.C. § 2000ee-1 (f)(1),(2).

([107]) Parecer 1/2016 do grupo de trabalho do artigo 29.º sobre a proteção de dados, sobre o projeto de decisão de adequação sobre o Escudo de Proteção da Privacidade UE-EUA (adotado em 13 de abril de 2016), p. 41.

([108]) Declarações do ODNI (anexo VI), p. 7. Ver, por exemplo, NSA, PPD-28 Secção 4 Procedimentos, 12 de janeiro de 2015, Sec. 8.1(c); CIA, *Signals Intelligence Activities, p. 7 (Responsibilities)*.

([109]) Este inspetor-geral (IG) (que foi criado em outubro de 2010) é nomeado pelo Presidente, confirmado pelo Senado e pode ser destituído apenas pelo Presidente e não pelo DNI.

([110]) O cargo destes inspetores-gerais é assegurado e só podem ser destituídos pelo Presidente, que deve comunicar ao Congresso, por escrito, os motivos da destituição. Tal não significa necessariamente que estão completamente isentos de instruções. Em alguns casos, o chefe do departamento pode proibir o inspetor-geral de iniciar, realizar ou concluir uma auditoria ou investigação em que tal seja considerado necessário para preservar interesses nacionais importantes (em matéria de segurança). Contudo, o Congresso deve ser informado do exercício desta autoridade e, com base no que precede, poderia responsabilizar o respetivo diretor. Ver, por exemplo, *Inspector General Act* de 1978, § 8 (IG do *Department of Defense*); § 8E (IGdo DOJ), § 8G (d)(2)(A),(B) (IG da NSA); 50. U.S.C. § 403q (b) (IG da CIA); *Intelligence Authorization Act For Fiscal Year 2010*, Sec. 405(f) (IG do setor das informações). Segundo a avaliação das autoridades nacionais de proteção dos dados, os inspetores-gerais «satisfarão provavelmente o critério relativo à independência organizacional tal como definida pelo TJUE e pelo Tribunal Europeu dos Direitos do Homem (TEDH), pelo menos a partir do momento em que o novo processo de nomeação seja aplicável a todos.» Veo o Parecer 1/2016 do grupo de trabalho do artigo 29.º sobre a proteção de dados, sobre o projeto de decisão de adequação sobre o Escudo de Proteção da Privacidade UE-EUA (adotado em 13 de abril de 2016), p. 40.

([111]) Ver declarações do ODNI (anexo VI), p. 7. Ver também *Inspector General Act* de 1978, com as alterações que lhe foram introduzidas, Pub. L. 113-126 de 7 de julho de 2014.

a todos os registos, relatórios, auditorias, revisões, documentos, recomendações ou outros materiais relevantes, através de intimações, se necessário, e podem recolher depoimentos ([112]). Embora os inspetores-gerais apenas possam emitir recomendações não vinculativas sobre medidas corretivas, os seus relatórios, nomeadamente sobre ações de acompanhamento (ou a sua inexistência) são publicados e, além disso, transmitidos ao Congresso que pode, com base neles, exercer a sua função de supervisão ([113]).

(98) Além disso, são atribuídas à *Privacy and Civil Liberties Oversight Board*, um órgão independente ([114]) dentro do poder executivo constituído por um conselho bipartidário de cinco membros ([115]) nomeados pelo Presidente para um mandato de seis anos e aprovados pelo Senado, responsabilidades no domínio das políticas de luta contra o terrorismo e da respetiva aplicação, com vista à proteção da privacidade e das liberdades cívicas. No quadro da sua análise da ação do setor das informações, pode aceder a todos os registos, relatórios, auditorias, análises, documentos e recomendações dos serviços de informações, nomeadamente informações classificadas, realizar entrevistas e recolher depoimentos. Recebe relatórios dos agentes responsáveis pela proteção da privacidade e das liberdades cívicas de vários departamentos/serviços federais ([116]), pode emitir recomendações e comunica regularmente aos comités do Congresso e ao Presidente ([117]). A PCLOB é igualmente responsável, dentro dos limites do seu mandato, pela preparação de um relatório de avaliação da aplicação da PPD-28.

(99) Por último, os mecanismos de supervisão supracitados são complementados pela *Intelligence Oversight Board* criada no âmbito do *Intelligence Advisory Board* do Presidente que supervisiona a conformidade dos serviços de informações dos EUA com a Constituição e todas as normas aplicáveis.

(100) Para facilitar a supervisão, os elementos do setor das informações são incentivados a conceber sistemas de informações que permitam o controlo, o registo e a análise das consultas ou outras pesquisas de informações pessoais ([118]). Os organismos de supervisão e conformidade verificarão periodicamente as práticas dos elementos do setor das informações para proteger as informações pessoais constantes da informação de origem eletromagnética e a sua conformidade com estes procedimentos ([119]).

(101) Além disso, estas funções de supervisão são apoiadas por amplos requisitos de comunicação no que diz respeito ao incumprimento. Em especial, os procedimentos dos serviços devem garantir que, sempre que se verifique um problema de conformidade grave que implique as informações pessoais de qualquer pessoa, independentemente da sua nacionalidade, recolhidas através de informação de origem eletromagnética, esse problema deve ser imediatamente comunicado ao chefe do elemento do setor das informações que, nos termos da PPD-28, deve determinar se são necessárias medidas corretivas ([120]). Além disso, de acordo com o Decreto Executivo n.º 12333, todos os elementos do setor das informações são obrigados a comunicar as situações de incumprimento à *Intelligence Oversight Board* ([121]). Estes mecanismos asseguram que o problema será resolvido no nível mais elevado

([112]) Ver *Inspector General Act* de 1978, § 6.
([113]) Ver declarações do ODNI (anexo VI), p. 7. Ver também *Inspector General Act* de 1978, §§ 4(5), 5. De acordo com a secção 405(b)(3),(4) da *Intelligence Authorization Act For Fiscal Year 2010*, Pub. L. 111-259 de 7 de outubro de 2010, o inspetor-geral do setor das informações manterá o DNI e o Congresso informados da necessidade e do progresso das medidas corretivas.
([114]) Segundo a avaliação das autoridades nacionais de proteção dos dados, a PCLOB demonstrou no passado «os seus poderes independentes». Ver o Parecer 1/2016 do grupo de trabalho do artigo 29.º sobre a proteção de dados, sobre o projeto de decisão de adequação sobre o Escudo de Proteção da Privacidade UE-EUA (adotado em 13 de abril de 2016), p. 42.
([115]) Além disso, a PCLOB emprega cerca de 20 funcionários regulares. Ver https://www.pclob.gov/about-us/staff.html.
([116]) Estes incluem, pelo menos, o *Department of Justice*, o *Department of Defense*, o *Department of Homeland Security*, o *Director of National Intelligence* e a *Central Intelligence Agency*, para além de qualquer outro departamento, serviço ou elemento do poder executivo que seja designado pela PCLOB por ser adequado para efeitos de abrangência.
([117]) Ver 42 U.S.C. § 2000ee. Ver também o mecanismo de mediação (anexo III), secção 6, alínea b), subalínea ii). Entre outras coisas, a PCLOB deverá informar quando uma agência do poder executivo se recusar a seguir o seu conselho.
([118]) ODNI, *Safeguarding the Personal Information of all People: A Status Report on the Development and Implementation of Procedures under Presidential Policy Directive 28*, p. 7-8.
([119]) Id. p. 8. Ver também declarações do ODNI (anexo VI), p. 9.
([120]) ODNI, *Safeguarding the Personal Information of all People: A Status Report on the Development and Implementation of Procedures under Presidential Policy Directive 28*, p. 7. Ver, por exemplo, NSA, PPD-28 Secção 4 Procedimentos, 12 de janeiro de 2015, Sec. 7.3, 8.7(c),(d); FBI, *Presidential Policy Directive 28 Policies and Procedures*, Sec. III (A)(4), (B)(4); CIA, *Signals Intelligence Activities*, p. 6 (*Compliance*) e p. 8 (*Responsibilities*).
([121]) Ver E.O. 12333, secção 1.6(c).

do setor das informações. Sempre que diga respeito a um cidadão de um país terceiro, o *Director of National Intelligence*, em consulta com o Secretary of State e o chefe do departamento ou serviço que efetua a notificação, deve determinar se devem ser tomadas medidas para notificar o governo estrangeiro em questão, em consonância com a proteção das fontes, dos métodos e dos funcionários dos EUA ([122]).

(102) Em segundo lugar, para além destes mecanismos de supervisão no poder executivo, o Congresso dos EUA, especificamente os *House and Senate Intelligence and Judiciary Committees*, tem responsabilidades de supervisão no que se refere a todas as atividades de informações externas dos EUA, designadamente a informação de origem eletromagnética. De acordo com a *National Security Act* (lei relativa à segurança nacional), «[o] Presidente deve garantir que os comités de informações do Congresso são mantidos plenamente informados e atualizados sobre as atividades de informações dos Estados Unidos, nomeadamente sobre qualquer atividade de informação prevista significativa, tal como exigido pelo presente subcapítulo» ([123]). Além disso, «[o] Presidente deve assegurar que todas as atividades de informações ilegais são imediatamente comunicadas aos comités de informações do Congresso, a par de todas as medidas corretivas tomadas ou previstas em relação a tal atividade ilegal» ([124]). Os membros destes comités têm acesso a informações classificadas, bem como a métodos e programas de informações ([125]).

(103) Legislação posterior alargou e aperfeiçoou os requisitos de comunicação, tanto relativamente aos elementos do setor das informações, como aos inspetores-gerais e ao *Attorney General*. Por exemplo, a FISA exige que o *Attorney General* «informe na íntegra» o Senado e os *House Intelligence and Judiciary Committees* relativamente às atividades do governo nos termos de determinadas secções da FISA ([126]). Exige ainda que o governo apresente aos comités do Congresso cópias de «todas as decisões, decretos ou pareceres do *Foreign Intelligence Surveillance Court* ou do *Foreign Intelligence Surveillance Court of Review* que incluam construção ou interpretação significativas» das disposições da FISA. Nomeadamente, no que se refere à vigilância nos termos da secção 702 da FISA, a supervisão é exercida através de relatórios exigidos por lei apresentados aos *Intelligence and Judiciary Committees*, bem como de esclarecimentos e audições frequentes. Estes incluem um relatório semestral apresentado pelo *Attorney General* que descreve a utilização da secção 702 da FISA, com documentos de apoio que incluem, nomeadamente os relatórios de conformidade do *Department of Justice* e do ODNI, bem como uma descrição de todas as situações de incumprimento ([127]), e uma avaliação semestral distinta efetuada pelo *Attorney General* e o DNI que documenta a conformidade com os procedimentos de orientação e minimização que visam garantir que a recolha é efetuada para atingir um objetivo válido em termos de informações externas ([128]). O Congresso também recebe relatórios elaborados pelos inspetores-gerais que estão autorizados a avaliar a conformidade dos serviços com os procedimentos de orientação e minimização, bem como com as orientações do *Attorney General*.

(104) De acordo com a *Freedom Act* de 2015, o governo dos EUA deve divulgar anualmente ao Congresso (e ao público) o número de decisões e diretivas solicitadas e recebidas ao abrigo da FISA, bem como as estimativas do número de cidadãos norte-americanos e de países terceiros que são alvo de vigilância, entre outros ([129]). A referida lei exige igualmente a comunicação pública adicional do número de NSL emitidas, novamente no que

([122]) PPD-28, secção 4(a)(iv).
([123]) Ver Sec. 501(a)(1) (50 U.S.C. § 413(a)(1)). Esta disposição contém os requisitos gerais no que se refere à supervisão efetuada pelo Congresso no domínio da segurança nacional.
([124]) Ver Sec. 501(b) (50 U.S.C. § 413(b)).
([125]) Ver Sec. 501(d) (50 U.S.C. § 413(d)).
([126]) Ver 50 U.S.C. §§ 1808, 1846, 1862, 1871, 1881f.
([127]) Ver 50 U.S.C. § 1881f.
([128]) Ver 50 U.S.C. § 1881a(l)(1).
([129]) Ver *USA Freedom Act* de 2015, Pub. L. N.º 114-23, Sec. 602(a). Além disso, segundo a secção 402, «o *Director of National Intelligence*, em consulta com o *Attorney General*, deve realizar uma reapreciação de desclassificação de cada decisão ou parecer emitido pelo *Foreign Intelligence Surveillance Court* ou o *Foreign Intelligence Surveillance Court of Review* (tribunal encarregado de apreciar os recursos relativos aos pedidos e mandatos em matéria de vigilância — tal como definido na secção 601(e)) que inclua uma construção ou interpretação significativa de qualquer disposição da legislação, incluindo qualquer interpretação ou construção nova ou significativa da expressão «termo de seleção específico» e, em consonância com essa reapreciação, disponibilizar ao público, tanto quanto possível, cada um destes pareceres ou decisões».

diz respeito aos cidadãos norte-americanos e de países terceiros (permitindo ao mesmo tempo que os destinatários de decisões e certificações nos termos da FISA, bem como de pedidos NSL, emitam relatórios de transparência em determinadas condições) ([130]).

(105) Em terceiro lugar, as atividades de informações levadas a cabo pelas autoridades públicas dos EUA com base na FISA permitem a reapreciação, e, em alguns casos, a autorização prévia das medidas pelo *Tribunal da FISA* (FISC) ([131]), um tribunal independente ([132]) cujas decisões podem ser impugnadas perante o *Foreign Intelligence Court of Review* (FISCR) ([133]) e, em última instância, o Supremo Tribunal dos Estados Unidos ([134]). Em caso de autorização prévia, as autoridades requerentes (FBI, NSA, CIA, etc.) terão de apresentar um projeto de pedido aos advogados do *National Security Department* do *Department of Justice* que analisarão e, se necessário, solicitarão informações adicionais ([135]). Após a finalização do pedido, este terá de ser aprovado pelo *Attorney General*, *Deputy Attorney General* ou pelo *Assistant Attorney General for National Security* ([136]). Subsequentemente, o *Department of Justice* apresentará o pedido ao FISC, que avaliará o pedido e emitirá uma determinação preliminar sobre a forma de proceder ([137]). Sempre que ocorra uma audição, o FISC tem autoridade para recolher depoimentos que podem incluir pareceres de peritos ([138]).

(106) O FISC (e o FISCR) são apoiados por um grupo permanente de cinco peritos em questões de segurança nacional, bem como em liberdades cívicas ([139]). A partir deste grupo, o tribunal deve nomear uma pessoa para intervir na qualidade de *amicus curiae*, a fim de assistir na análise de qualquer pedido de decisão ou reapreciação que, na opinião do tribunal, apresente uma interpretação nova ou significativa do direito, a menos que o tribunal considere que tal nomeação não é adequada ([140]). Em especial, tal deve garantir que as considerações em matéria de proteção da privacidade são tidas em devida conta na avaliação do tribunal. O tribunal também pode nomear uma pessoa ou organização para intervir na qualidade de *amicus curiae*, fornecendo, nomeadamente, competências técnicas, sempre que considere necessário ou, mediante pedido, autorizar uma pessoa ou organização a apresentar informações a título de *amicus curiae* ([141]).

([130]) *USA Freedom Act*, Sec. 602(a), 603(a).

([131]) No que se refere a determinados tipos de vigilância, em alternativa, um magistrado dos EUA publicamente designado pelo *Chief Justice* dos Estados Unidos pode ter competência para apreciar pedidos e emitir decisões.

([132]) O FISC é constituído por onze juízes nomeados pelo *Chief Justice* a partir dos juízes em funções nos tribunais distritais dos EUA, que foram previamente nomeados pelo Presidente e confirmados pelo Senado. Os juízes, que dispõem de um posto vitalício, só podendo ser destituídos por justa causa, exercem funções no FISC durante mandatos alternados de sete anos. A FISA exige que os juízes sejam selecionados a partir de, pelo menos, sete círculos judiciais diferentes dos EUA. Ver Sec. 103 FISA (50 U.S.C. 1803 (a)); PCLOB, Sec. 215 Report, p. 174-187. Os juízes são apoiados por referendários experientes que constituem os especialistas jurídicos do tribunal e preparam a análise jurídica relativa aos pedidos de recolha. Ver PCLOB, Sec. 215 Report, p. 178; Carta do Excelentíssimo Senhor Reggie B. Walton, juiz presidente, *Foreign Intelligence Surveillance Court* dos EUA, ao Excelentíssimo Senhor Patrick J. Leahy, Presidente, *Committee on the Judiciary*, Senado dos EUA (29 de julho de 2013) («Carta de Walton»), p. 2-3.

([133]) O FISCR é constituído por três juízes nomeados pelo *Chief Justice* dos Estados Unidos e selecionados a partir dos tribunais distritais ou tribunais de recurso dos EUA, exercendo funções durante um mandato intercalado de sete anos. Ver Sec. 103 FISA (50 U.S.C. § 1803 (b)).

([134]) Ver 50 U.S.C. §§ 1803 (b), 1861 a (f), 1881 a (h), 1881 a (i)(4).

([135]) Por exemplo, dados factuais adicionais sobre o alvo da vigilância, informações técnicas sobre a metodologia de vigilância ou garantias sobre como as informações obtidas serão utilizadas e divulgadas. Ver PCLOB, Sec. 215 *Report*, p. 177.

([136]) 50 U.S.C. §§ 1804 (a), 1801 (g).

([137]) O FISC pode aprovar o pedido, solicitar informações adicionais, determinar a necessidade de uma audição ou indicar uma possível recusa do pedido. Com base nesta determinação preliminar, o governo apresentará o seu pedido final. Este último pode incluir alterações significativas ao pedido inicial com base nas observações preliminares do juiz. Embora uma percentagem elevada de pedidos finais seja aprovada pelo FISC, uma parte significativa destes contém alterações substantivas ao pedido inicial, por exemplo, 24 % dos pedidos aprovados entre julho e setembro de 2013. Ver PCLOB, Sec. 215 Report, p. 179; Carta de Walton, p. 3.

([138]) PCLOB, Sec. 215 Report, p.179, n.º 619.

([139]) 50 U.S.C. § 1803 (i)(1),(3)(A). Esta nova legislação implementou recomendações apresentadas pela PCLOB com vista a criar um grupo de peritos em questões de proteção da privacidade e das liberdades cívicas que possa intervir na qualidade de *amicus curiae*, a fim de fornecer ao tribunal os argumentos jurídicos conducentes ao aumento da proteção da privacidade e das liberdades cívicas. Ver PCLOB, Sec. 215 Report, p. 183-187.

([140]) 50 U.S.C. § 1803 (i)(2)(A). De acordo com as informações apresentadas pelo ODNI, tais nomeações já ocorreram. Ver *Signals Intelligence Reform, 2016 Progress Report*.

([141]) 50 U.S.C. § 1803 (i)(2)(B).

(107) No que se refere às duas autorizações judiciais de vigilância nos termos da FISA que são mais importantes para as transferências de dados ao abrigo do Escudo de Proteção da Privacidade UE-EUA, a supervisão pelo FISC difere.

(108) Nos termos da secção 501 da FISA ([142]), que permite a recolha de «todas as coisas tangíveis (nomeadamente livros, registos, documentos e outros elementos)», o pedido apresentado junto do FISC deve conter uma declaração dos factos que demonstre que existem motivos razoáveis para considerar que as coisas tangíveis solicitadas são relevantes para uma investigação autorizada (que não uma avaliação das ameaças) realizada para obter informações no estrangeiro não relacionadas com um cidadão norte-americano ou para efeitos de proteção contra o terrorismo internacional ou atividades de informações clandestinas. Além disso, o pedido deve conter uma enumeração dos procedimentos de minimização adotados pelo *Attorney General* para a preservação e divulgação das informações recolhidas ([143]).

(109) Pelo contrário, nos termos da secção 702 da FISA ([144]), o FISC não autoriza medidas de vigilância individuais; em vez disso, autoriza programas de vigilância (tais como o PRISM e o UPSTREAM) com base em certificações anuais elaboradas pelo *Attorney General* e o *Director of National Intelligence*. A secção 702 da FISA permite que se visem pessoas que se acredite estarem localizadas fora dos Estados Unidos a fim de obter informações no estrangeiro ([145]). Esta seleção da pessoa visada é realizada pela NSA em duas fases: em primeiro lugar, os analistas da NSA identificaram os cidadãos de países terceiros localizados no estrangeiro cuja vigilância conduzirá, com base na avaliação do analista, às informações externas relevantes especificadas na certificação. Em segundo lugar, após a identificação destas pessoas e a sua aprovação como objetivos por um amplo mecanismo de análise no âmbito da NSA ([146]), são designados (ou seja, desenvolvidos e aplicados) os seletores que identificam os meios de comunicação (como o endereço de correio eletrónico) utilizados pelas pessoas visadas ([147]). Tal como indicado, as certificações a aprovar pelo FISC não contêm informações sobre as pessoas visadas, mas sim categorias de identificação das informações no estrangeiro ([148]). Embora o FISC não avalie — com base numa causa provável ou em qualquer outra norma — se as pessoas são adequadamente visadas para efeitos de obtenção de informações externas ([149]), o seu controlo alarga-se à condição de que «um objetivo significativo da recolha consiste na obtenção de informações no estrangeiro» ([150]). Com efeito, nos termos da secção 702 do FISA, a NSA pode recolher comunicações de cidadãos de países terceiros fora dos EUA apenas se for possível considerar razoavelmente que um determinado meio de comunicação está a ser utilizado para comunicar informações no estrangeiro (por exemplo, relacionadas com terrorismo internacional, proliferação nuclear ou atividades cibernéticas hostis). As determinações para este efeito são objeto de controlo jurisdicional ([151]). As certificações também necessitam de prever procedimentos de orientação e minimização ([152]). O *Attorney General* e o *Director of*

([142]) 50 U.S.C. § 1861.
([143]) 50 U.S.C. § 1861 (b).
([144]) 50 U.S.C. § 1881.
([145]) 50 U.S.C. § 1881a (a).
([146]) PCLOB, Sec. 702 *Report*, p. 46.
([147]) 50 U.S.C. § 1881a (h).
([148]) 50 U.S.C. § 1881a (g). De acordo com a PCLOB, até à data, estas categorias dizem respeito sobretudo ao terrorismo internacional e a temas como a aquisição de armas de destruição maciça. Ver PCLOB, Sec. 702 *Report*, p. 25.
([149]) PCLOB, Sec. 702 *Report*, p. 27.
([150]) 50 U.S.C. § 1881a.
([151]) «*Liberty and Security in a Changing World*», *Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies*, 12 de dezembro de 2013, p. 152.
([152]) 50 U.S.C.1881a (i).

National Intelligence verificam a conformidade e os serviços são obrigados a comunicar todas as situações de incumprimento ao FISC ([153]) (bem como ao Congresso e à *Intelligence Oversight Board* do Presidente), que, com base no que precede, pode alterar a autorização ([154]).

(110) Além disso, a fim de aumentar a eficiência da supervisão pelo FISC, a administração dos EUA concordou em implementar uma recomendação apresentada pela PCLOB com o objetivo de fornecer ao FISC documentação relativa às decisões sobre a seleção de alvos nos termos da secção 702, designadamente uma amostra aleatória de formulários de atribuição de missões, para permitir ao FISC avaliar de que modo o requisito para efeitos de informações externas é cumprido na prática ([155]). Ao mesmo tempo, a administração dos EUA aceitou e tomou medidas para rever os procedimentos de seleção de alvos da NSA para documentar melhor os motivos para a recolha de informações externas apresentados nas decisões relativas à seleção de alvos ([156]).

Reparação individual

(111) Existem várias vias acessíveis nos termos da legislação dos EUA aos titulares de dados da UE caso estes tenham preocupações relativamente à possibilidade de os seus dados pessoais terem sido tratados (recolhidos, avaliados, etc.) por elementos do setor das informações dos EUA, e em caso positivo, se as limitações aplicáveis na legislação dos EUA foram cumpridas. Essencialmente estas dizem respeito a três domínios: ingerência nos termos da FISA; acesso ilegal e intencional aos dados pessoais por parte de funcionários do governo; e acesso à informação nos termos da *Freedom of Information Act* (lei relativa à liberdade de informação — FOIA) ([157]).

(112) Em primeiro lugar, a *Foreign Intelligence Surveillance Act* prevê várias vias de recurso acessíveis igualmente a cidadãos de países terceiros, a fim de contestar a vigilância eletrónica ilegal ([158]). O que precede inclui a possibilidade de as pessoas instaurarem uma ação civil de indemnização contra os Estados Unidos sempre que as informações sobre si tenham sido ilegal e intencionalmente utilizadas ou divulgadas ([159]); instaurarem uma ação de indemnização contra funcionários do governo dos EUA na sua capacidade pessoal («no aparente cumprimento da lei») ([160]); e contestarem a legalidade da vigilância (e solicitarem a supressão das informações) caso o governo dos EUA tencione utilizar ou divulgar quaisquer informações obtidas ou decorrentes de vigilância eletrónica contra a pessoa em processos judiciais ou administrativos nos Estados Unidos ([161]).

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

([153]) A regra 13, alínea b), do regulamento interno do FISC exige que o governo informe o Tribunal, por escrito, imediatamente após a descoberta de que uma autorização ou aprovação concedida pelo Tribunal foi implementada de forma contrária à autorização ou aprovação do Tribunal, ou à legislação aplicável. Exige ainda que o governo notifique o tribunal por escrito dos factos e circunstâncias relevantes para tal incumprimento. Normalmente, o governo apresentará uma notificação final relativa à regra 13, alínea a), depois de tomar conhecimento dos factos relevantes e da destruição de todas as informações decorrentes da recolha não autorizada. Ver *Walton Letter*, p. 10.

([154]) 50 U.S.C. § 1881 (l). Ver também PCLOB, Sec. 702 Report, p. 66-76; *NSA CLPO, NSA's Implementation of Foreign Intelligence Surveillance Act Section 702*, 16.4.2014. A recolha de dados pessoais para efeitos de informações nos termos da secção 702 da FISA é objeto de supervisão interna e externa no seio do poder executivo. Entre outros, a supervisão interna inclui programas de conformidade interna para avaliar e supervisionar a conformidade com os procedimentos de orientação e minimização; comunicação de situações de incumprimento, tanto a nível interno como externo ao ODNI, ao *Department of Justice*, ao Congresso e ao FISC; e reapreciações anuais transmitidas aos mesmos organismos. No que se refere à supervisão externa, esta é constituída sobretudo por análises de orientação e minimização realizadas pelo ODNI, o DOJ, e os inspetores-gerais, que, por sua vez, comunicam ao Congresso e a FISC, designadamente sobre situações de incumprimento. As situações de incumprimento graves devem ser imediatamente comunicadas ao FISC e as restantes devem ser comunicadas num relatório trimestral. Ver PCLOB, Sec. 702 *Report*, p. 66-77.

([155]) PCLOB, *Recommendations Assessment Report*, 29.1.2015, p. 20.

([156]) PCLOB, *Recommendations Assessment Report*, 29.1.2015, p. 16.

([157]) Além disso, a secção 10 da *Classified Information Procedures Act* (lei relativa ao processo aplicável às informações classificadas) prevê que, em qualquer ação judicial na qual os Estados Unidos devam determinar que o material constitui informações classificadas (por exemplo, porque necessita de proteção contra a divulgação não autorizada por motivos de segurança nacional), os Estados Unidos devem notificar o requerido das partes do material nas quais espera razoavelmente basear-se para estabelecer o elemento das informações classificadas da infração.

([158]) Ver as seguintes declarações do ODNI (anexo VI), p. 16.

([159]) 18 U.S.C. § 2712.

([160]) 50 U.S.C. § 1810.

([161]) 50 U.S.C. § 1806.

nacional (isto é, a *Computer Fraud and Abuse Act* ([162]); a *Electronic Communications Privacy Act* ([163]); e a *Right to Financial Privacy Act* ([164])). Todas estas ações são referentes a dados, alvos e/ou tipos de acesso específicos (por exemplo, acesso remoto a um computador através da Internet) e encontram-se disponíveis em determinadas condições (por exemplo, conduta intencional/deliberada, conduta fora da capacidade oficial, danos sofridos) ([165]). Uma possibilidade mais geral de recurso está prevista na *Administrative Procedure Act* (5 U.S.C. § 702), segundo a qual «qualquer pessoa que sofra um prejuízo resultante de uma decisão de uma agência ou que é afetada ou lesada pela decisão de uma agência», pode interpor um recurso judicial. Tal inclui a possibilidade de solicitar ao tribunal «que declare ilegais e anule a atuação, os resultados e as conclusões da agência, que se venham a verificar […] arbitrários, caprichosos, um abuso de poder, ou de outro modo não conformes ao direito» ([166]).

(114) Por último, o governo dos EUA salientou a FOIA como um meio para os cidadãos de países terceiros solicitarem o acesso a documentação existente dos serviços federais, nomeadamente nos casos em que esta contenha os dados pessoais do respetivo titular ([167]). Devido à sua incidência, a FOIA não prevê uma via de recurso individual contra a ingerência nos dados pessoais como tal, embora possa, em princípio, permitir que as pessoas obtenham acesso a informações relevantes conservadas por serviços de informações nacionais. Mesmo a este respeito, as possibilidades parecem ser limitadas, uma vez que os serviços podem reter informações abrangidas por determinadas exceções enumeradas, nomeadamente o acesso a informações de segurança nacional classificadas e informações relativas a investigações relacionadas com a aplicação da lei ([168]). Tomando em consideração o que precede, a utilização de tais exceções pelos serviços de informações nacionais pode ser contestada pelas pessoas, que podem solicitar o controlo jurisdicional e administrativo.

(115) Embora as pessoas, incluindo os titulares de dados da UE, disponham de várias vias de recurso se tiverem sido objeto de vigilância (eletrónica) ilegal para efeitos de segurança nacional, é igualmente evidente que pelo menos algumas bases jurídicas que os serviços de informações dos EUA podem utilizar (por exemplo E.O. 12333) não são abrangidas. Além disso, mesmo nos casos em que, em princípio, existem possibilidades de recurso judicial para cidadãos de países terceiros, como no que diz respeito à vigilância ao abrigo da FISA, as causas de ação disponíveis são limitadas ([169]) e as ações apresentadas por pessoas singulares (incluindo cidadãos dos EUA) serão declaradas inadmissíveis se não conseguirem demonstrar «legitimidade» ([170]), o que limita o acesso aos tribunais comuns ([171]).

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

([162]) 18 U.S.C. § 1030.
([163]) 18 U.S.C. §§ 2701-2712.
([164]) 12 U.S.C. § 3417.
([165]) Declarações do ODNI (anexo VI), p. 17.
([166]) 5 U.S.C. § 706(2)(A).
([167]) 5 U.S.C. § 552. Existem leis semelhantes a nível estadual.
([168]) Caso tal se verifique, em regra, a pessoa receberá apenas uma resposta-padrão através da qual o serviço não confirma nem desmente a existência de qualquer documentação. Ver *ACLU v. CIA*, 710 F.3d 422 (D.C. Cir. 2014).
([169]) Ver declarações do ODNI (anexo VI), p. 16. De acordo com as explicações apresentadas, as causas de ação disponíveis exigem a existência de *danos* (18 U.S.C. § 2712; 50 U.S.C. § 1810) ou uma demonstração de que o *governo pretende utilizar ou divulgar informações* obtidas ou decorrentes de vigilância eletrónica do titular dos dados contra essa pessoa *em processos judiciais ou administrativos* nos Estados Unidos (50 U.S.C. § 1806). Contudo, tal como o Tribunal de Justiça salientou repetidamente, para determinar a existência de uma ingerência no direito fundamental à privacidade, é indiferente se o titular dos dados sofreu consequências adversas em virtude dessa ingerência. Ver *Schrems*, n.º 89 com referências adicionais.
([170]) Este critério de admissibilidade advém do requisito de «caso ou controvérsia» da Constituição dos EUA, artigo III.
([171]) Ver *Clapper v. Amnesty Int'l USA*, 133 S.Ct. 1138, 1144 (2013). No que se refere à utilização de NSL, a *Freedom Act* (secção 502(f)-503) prevê que os requisitos de não divulgação devem ser periodicamente reexaminados e que os *destinatários* de NSL devem ser notificados sempre que os factos deixem de apoiar um requisito de não notificação (ver declarações do ODNI (anexo VI), p. 13). Contudo, tal não garante que o titular de dados da UE seria informado de que foi objeto de uma investigação.

(117) Em especial, de acordo com os compromissos do governo dos EUA, o mecanismo de mediação assegurará que as queixas individuais são investigadas e abordadas de forma adequada e que as pessoas recebem uma confirmação independente de que as leis dos EUA foram cumpridas ou, no caso de uma violação dessas leis, que o incumprimento foi corrigido ([172]). O mecanismo inclui «o Mediador para o Escudo de Proteção da Privacidade», ou seja, o *Under-Secretary* e outro pessoal, assim como outros órgãos de supervisão competentes para controlar os diversos elementos dos serviços de informação em cuja cooperação o Mediador para o Escudo de Proteção da Privacidade se baseará para tratar das queixas. Em especial, quando o pedido de uma pessoa se refira à compatibilidade da vigilância com a legislação americana, o Mediador para o Escudo de Proteção da Privacidade poderá confiar em organismos de supervisão independentes com competências de investigação (como os inspetores-gerais e a PCLOB). Em cada caso, o *Secretary of State* garantirá que o Mediador disporá dos meios para assegurar que a sua resposta aos pedidos individuais se baseie em todas as informações necessárias.

(118) Através desta «estrutura composta», o mecanismo de mediação garante uma supervisão independente e um recurso individual. Além disso, a cooperação com outros organismos de supervisão assegura o acesso aos conhecimentos especializados necessários. Por último, ao impor ao Mediador para o Escudo de Proteção da Privacidade a obrigação de confirmar o cumprimento ou a correção de um incumprimento, o mecanismo reflete um compromisso do governo dos EUA no seu conjunto de tratar e resolver as queixas apresentadas por cidadãos da UE.

(119) Em primeiro lugar, ao contrário de um mecanismo exclusivamente intragovernamental, o Mediador para o Escudo de Proteção da Privacidade receberá e responderá a queixas individuais. Tais queixas podem ser dirigidas às autoridades de supervisão dos Estados-Membros competentes em matéria de supervisão dos serviços de segurança nacional e/ou do tratamento dos dados pessoais pelas autoridades públicas, que as apresentarão a um organismo centralizado a nível da UE, que as enviará ao Mediador para o Escudo de Proteção da Privacidade ([173]). Com efeito, tal beneficiará os cidadãos da UE, que podem recorrer a uma autoridade nacional «perto de casa» e na própria língua. A função de tal autoridade consistirá em apoiar o cidadão na apresentação de um pedido junto do Mediador para o Escudo de Proteção da Privacidade que contém as informações de base podendo, assim, ser considerado «completo». A pessoa não tem de demonstrar que o governo dos EUA acedeu, de facto, aos seus dados pessoais através de atividades de informação de origem eletromagnética.

(120) Em segundo lugar, o governo americano compromete-se a garantir que, no exercício das suas funções, o Mediador para o Escudo de Proteção da Privacidade poderá apoiar-se na cooperação de outros mecanismos de verificação do cumprimento e de supervisão previstos no direito dos EUA. Tal implicará por vezes os serviços de informações nacionais, em especial se o pedido tiver de ser interpretado como um pedido de acesso a documentos relacionados com a *Freedom of Information Act*. Noutros casos, em especial quando os pedidos dizem respeito à compatibilidade da vigilância com a legislação dos EUA, tal cooperação implicará organismos de supervisão independentes (por exemplo, inspetores-gerais) com a responsabilidade e poder para realizar uma investigação aprofundada (em especial através do acesso a todos os documentos pertinentes e competência para solicitar informações e declarações) e abordar casos de incumprimento ([174]). Além disso, o Mediador para o Escudo de Proteção da Privacidade terá a capacidade de submeter questões à PCLOB para análise ([175]). Nos casos em que um destes organismos de supervisão tenha detetado qualquer incumprimento, os serviços de informação em questão (por exemplo, uma agência de informações) terá de corrigir o incumprimento, uma vez que apenas

([172]) Se o queixoso procurar ter acesso a documentos na posse das autoridades públicas dos EUA, são aplicáveis as regras e os procedimentos descritos na *Freedom of Information Act*. Tal inclui a possibilidade de interpor um recurso judicial (em vez de uma supervisão independente) no caso de o pedido ser rejeitado, em conformidade com as condições estabelecidas na FOIA.

([173]) De acordo com o mecanismo de mediação (anexo III), secção 4, alínea f), o Mediador para o Escudo de Proteção da Privacidade comunicará diretamente com o organismo responsável pela resolução de queixas dos cidadãos da UE que, por sua vez, será responsável por comunicar com a pessoa que apresenta o pedido. Se as comunicações diretas fizerem parte dos «processos subjacentes» passíveis de proporcionar a reparação solicitada (por exemplo, um pedido de acesso nos termos da FOIA, secção 5), essas comunicações verificar-se-ão em conformidade com os procedimentos aplicáveis.

([174]) Ver mecanismo de mediação (anexo III), secção 2, alínea a). Ver também considerandos 0-0.

([175]) Ver mecanismo de mediação (anexo III), secção 2, alínea c). De acordo com as explicações apresentadas pelo governo dos EUA, a PCLOB deve examinar continuamente os procedimentos e políticas, bem como a respetiva aplicação, das autoridades dos EUA responsáveis pela luta contra o terrorismo a fim de determinar se as suas ações «protegem de modo adequado a privacidade e as liberdades cívicas e são coerentes com a regulamentação, as políticas e as leis que regem a privacidade e as liberdades cívicas». Deve igualmente «receber e examinar relatórios e outras informações dos agentes responsáveis pela proteção da privacidade e das liberdades cívicas e, sempre que adequado, apresentar-lhes recomendações sobre as suas atividades».

deste modo o Mediador poderá garantir uma resposta «positiva» à pessoa (ou seja, que se corrigiu o incumprimento), em relação ao qual o governo americano se comprometeu. Por outro lado, no quadro da cooperação, o Mediador para o Escudo de Proteção da Privacidade será informado dos resultados da investigação, e disporá dos meios para garantir que recebe todas as informações necessárias para preparar a resposta.

(121) Por último, o Mediador para o Escudo de Proteção da Privacidade será um órgão independente e, como tal, não receberá instruções dos serviços de informações dos EUA ([176]). O que precede é especialmente importante, uma vez que o mediados terá de «confirmar» que i) a queixa foi devidamente investigada e que ii) a legislação dos EUA pertinente — nomeadamente as limitações e garantias estabelecidas no anexo VI — foi cumprida ou, em caso de incumprimento, que tal infração foi corrigida. A fim de poder fornecer esta confirmação independente, o Mediador para o Escudo de Proteção da Privacidade terá de receber as informações necessárias relativamente à investigação para avaliar a exatidão da resposta à queixa. Além disso, o *Secretary of State* comprometeu-se a garantir que o *Under-Secretary* desempenhará as funções de Mediador para o Escudo de Proteção da Privacidade de froma objetiva e sem quaisquer influências indevidas suscetíveis de terem um efeito na resposta a dar.

(122) Globalmente, este mecanismo assegura que as queixas individuais serão investigadas de forma aprofundada e tratadas, e que, pelo menos no domínio da vigilância, se recorra a organismos de supervisão independentes com as competências e os poderes de investigação necessários e um Mediador que possa exercer as suas funções sem quaisquer influências indevidas, especialmente a nível político. Além disso, as pessoas poderão apresentar queixas sem terem de demonstrar, ou mesmo fornecer elementos que indiquem que foram objeto de vigilância ([177]). Tendo em conta estes elementos, a Comissão congratula-se por ver que existem garantias adaptadas e eficazes contra os abusos.

(123) Tendo em conta tudo o que precede, a Comissão conclui que os EUA asseguram uma proteção jurídica eficaz contra as ingerências por parte dos seus serviços de informações nos direitos fundamentais das pessoas cujos dados são transferidos da União para os Estados Unidos ao abrigo do Escudo de Proteção da Privacidade UE-EUA.

(124) Relativamente a este aspeto, a Comissão toma nota do acórdão do Tribunal de Justiça proferido no processo *Schrems*, segundo o qual «uma regulamentação que não preveja nenhuma possibilidade de o particular recorrer a vias de direito para ter acesso aos dados pessoais que lhe dizem respeito, ou para obter a retificação ou a supressão de tais dados, não respeita o conteúdo essencial do direito fundamental a uma proteção jurisdicional efetiva, tal como é consagrado no artigo 47.º da Carta» ([178]). A avaliação da Comissão confirmou que tais vias de recurso estão previstas nos Estados Unidos, em especial através da introdução da figura do Mediador. Esta figura dispõe de poderes de supervisão independente com competências de investigação. No quadro da sua supervisão contínua do Escudo de Proteção da Privacidade, nomeadamente através da análise conjunta anual em que também participará o Mediador, a Comissão reapreciará a eficácia deste mecanismo.

3.2. *Acesso aos dados e respetiva utilização pelas autoridades públicas dos EUA para efeitos de garantir a aplicação da lei e outros fins de interesse público*

(125) No que diz respeito à ingerência nos dados pessoais transferidos ao abrigo do Escudo de Proteção da Privacidade UE-EUA para efeitos de aplicação da lei, o governo dos EUA (através do *Department of Justice*) apresentou garantias sobre as limitações e salvaguardas aplicáveis que, na avaliação da Comissão, demonstram um nível de proteção adequado.

([176]) Ver *Roman Zakharov/Rússia*, Acórdão de 4 de dezembro de 2015 (Grande Secção), Queixa n.º 47143/06, n.º 275 (embora seja em princípio desejável que a função de supervisão seja confiada a um juiz, podendo a supervisão efetuada por um órgão não judicial ser considerada compatível com a Convenção, desde que esse órgão de supervisão seja independente das autoridades que procedem à supervisão e seja investida de poderes e atribuições suficientes).

([177]) Ver *Kennedy/Reino Unido*, Acórdão de 18 de maio de 2010, Queixa n.º 26839/05, n.º 167.

([178]) *Schrems*, n.º 95. Como decorre dos n.ºs 91 e 96 do acórdão, o n.º 95 diz respeito ao nível de proteção garantido na ordem jurídica da União, ao qual o nível de proteção no país terceiro deve ser «essencialmente equivalente». Segundo os n.ºs 73 e 74 do acórdão, tal não significa que o nível de proteção ou os meios a que o país terceiro recorreu devam ser idênticos, mesmo que os meios utilizados devam provar, na prática, que são eficazes.

(126) De acordo com estas informações, nos termos da Quarta Emenda da Constituição dos EUA ([179]), as buscas e apreensões efetuadas pelas autoridades com funções coercivas ([180]) exigem principalmente um mandado judicial após a demonstração de uma «causa provável». Nos poucos casos excecionais e especificamente estabelecidos nos quais o requisito de um mandado não é aplicável ([181]), o exercício das funções coercivas é objeto de um teste de «razoabilidade» ([182]). Determina-se se uma busca ou apreensão é razoável «através da avaliação, por um lado, da medida em que invade a privacidade de uma pessoa e, por outro lado, da medida em que é necessária para a promoção de interesses governamentais legítimos» ([183]). Em termos mais gerais, a Quarta Emenda garante a privacidade, a dignidade e assegura a proteção contra atos arbitrários e invasivos por parte de funcionários do governo ([184]). Estes conceitos refletem a ideia de necessidade e proporcionalidade constante do direito da União. Quando as autoridades com funções coercivas já não precisam de utilizar os elementos apreendidos como provas, devem restituí-los ([185]).

(127) Embora o direito decorrente da Quarta Emenda não abranja os cidadãos de países terceiros não residentes nos Estados Unidos, estes últimos beneficiam, indiretamente da sua proteção, dado que são as empresas dos EUA que detêm dados pessoais, devendo as autoridades com funções coercivas em qualquer caso obter autorização judicial (ou pelo menos respeitar o requisito de razoabilidade ([186]). Outras salvaguardas decorrem de competências jurídicas especiais, bem como das orientações do *Department of Justice*, que limitam o acesso aos dados das autoridades com funções coercivas por motivos equivalentes à necessidade e proporcionalidade (por exemplo, exigindo que o FBI utilize os métodos de investigação menos invasivos possíveis, tomando em consideração o efeito sobre a privacidade e as liberdades cívicas) ([187]). Segundo as declarações apresentadas pelo governo dos EUA, são aplicáveis proteções idênticas ou mais elevadas às investigações das autoridades com funções coercivas a nível estadual (no que se refere às investigações executadas ao abrigo das leis estaduais) ([188]).

(128) Embora uma autorização judicial prévia concedida por um tribunal ou júri (um braço de investigação do tribunal reunido por um juiz ou magistrado) não seja necessária em todos os casos ([189]), as intimações administrativas estão limitadas a casos específicos e serão objeto de um controlo jurisdicional independente pelo menos nos casos em que o governo solicite uma execução em tribunal ([190]).

([179]) Nos termos da Quarta Emenda, o direito dos cidadãos à inviolabilidade de pessoas, casas, documentos e propriedade pessoal contra buscas e apreensões não razoáveis não deve ser violado, e não devem ser emitidos mandatos a não ser com causa provável apoiada por juramento ou declaração e descrevendo especificamente o local da busca e as pessoas ou coisas a serem apreendidas. Só os juízes (magistrados) podem emitir mandados de busca. Os mandados federais relativos à reprodução de informações armazenadas em suporte eletrónico são, além disso, regidas pelo artigo 41.º do Código Federal de Processo Penal).

([180]) O Tribunal Supremo já considerou em várias ocasiões as buscas sem mandado como «excecionais». Ver, por exemplo, *Johnson/Estados Unidos*, 333 U.S. 10, 14 (1948); Ver, por exemplo, *McDonald/*, 335 U.S. 451, 453 (1948); Ver, por exemplo, *Camara/Municipal Court*, 387 U.S. 523, 528 (1967); *G.M. Leasing Corp./Estados Unidos*, 429 U.S. 338, 352-53, 355 (1977). Do mesmo modo, o Supremo Tribunal sublinha periodicamente que a regra constitucional mais básica neste domínio é que as buscas realizadas fora do âmbito do processo judicial, sem autorização prévia do juiz ou magistrado, não são *per se* razoáveis ao abrigo da Quarta Emenda — sem prejuízo de algumas exceções especificamente estabelecidas e bem definidas. Ver, por exemplo, *Coolidge/New Hampshire*, 403 U.S. 443, 454-55 (1971); *G.M. Leasing Corp./Estados Unidos*, 429 U.S. 338, 352-53, 358 (1977).

([181]) *City of Ontario, Cal./Quon*, 130 S. Ct. 2619, 2630 (2010).

([182]) PCLOB, Sec. 215 Report, p. 107, que faz referência a *Maryland/King*, 133 S. Ct. 1958, 1970 (2013).

([183]) PCLOB, Sec. 215 Report, p. 107, que faz referência a *Samson/California*, 547 U.S. 843, 848 (2006).

([184]) *City of Ontario, Cal./Quon*, 130 S. Ct. 2619, 2630 (2010), 2627.

([185]) Ver, por exemplo, Estados Unidos/*Wilson*, 540 F.2d 1100 (D.C. Cir. 1976).

([186]) Ver *Roman Zakharov/Rússia*, Acórdão de 4.12.2015 (Grande Secção), Queixa n.º 47143/06, n.º 269, segundo o qual a condição de apresentar uma autorização de interceção ao fornecedor de serviços de comunicação para poder aceder às comunicações de uma pessoa constitui uma das garantias importantes contra os abusos por parte das autoridades com funções coercivas, garantindo que é obtida uma autorização adequada em todos os casos de interceção.

([187]) Declarações do DOJ (anexo VII), p. 4 com referências adicionais.

([188]) Declarações do DOJ (anexo VII), n.º 2.

([189]) De acordo com as informações que a Comissão recebeu, e não tomando em consideração domínios específicos provavelmente irrelevantes em matéria de transferência de dados ao abrigo do Escudo de Proteção da Privacidade UE-EUA (por exemplo, investigações sobre casos de fraude nos serviços de saúde, abuso de crianças ou substâncias controladas), tal diz respeito sobretudo a determinadas autoridades nos termos da *Electronic Communications Privacy Act* (ECPA), designadamente os pedidos de informações básicas sobre os assinantes, as sessões e a faturação (18 U.S.C. § 2703(c)(1), (2), por exemplo, endereço, tipo/duração do serviço) e os pedidos de acesso ao conteúdo de mensagens de correio eletrónico com mais de 180 dias (18 U.S.C. § 2703(b)). Contudo, neste último caso, o titular dos dados deve ser notificado tendo, portanto, a oportunidade de contestar o pedido em tribunal. Ver igualmente a visão do DOJ, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, Cap. 3: *The Stored Communications Act*, p. 115-138.

([190]) Segundo as declarações do governo dos EUA, os destinatários de intimações administrativas podem contestá-las em tribunal alegando que não são razoáveis, ou seja, que são demasiado amplas, opressivas ou onerosas. Ver declarações do DOJ (anexo VII), p. 2.

(129) O mesmo é aplicável à utilização de intimações administrativas para efeitos de interesse público. Além disso, de acordo com as declarações do governo dos EUA, são aplicáveis limitações substantivas semelhantes segundo as quais os serviços só podem solicitar o acesso a dados relevantes para questões abrangidas pelo seu âmbito de autoridade e devem respeitar a norma de razoabilidade.

(130) Além disso, a legislação dos EUA prevê um certo número de vias de recurso judiciais para as pessoas singulares, contra as autoridades públicas ou um dos seus funcionários, quando estas autoridades tratam dados pessoais. Estas vias, que incluem especialmente a *Administrative Procedure Act* (APA), a *Freedom of Information Act* (FOIA) e a *Electronic Communications Privacy Act* (ECPA), estão abertas a todas as pessoas independentemente da sua nacionalidade, sujeitassem prejuízo de quaisquer condições aplicáveis.

(131) Em geral, ao abrigo das disposições relativas a um recurso judicial da *Administrative Procedure Act* ([191]), «qualquer pessoa que sofra um prejuízo resultante de uma decisão de uma agência ou que é afetada ou lesada pela decisão de uma agência, pode int»erpor um recurso judicial ([192]). Tal inclui a possibilidade de solicitar ao tribunal «que declare ilegais e anule a atuação, os resultados e as conclusões da agência, que se venham a verificar […] arbitrários, caprichosos, um abuso de poder, ou de outro modo não conformes ao direito» ([193]).

(132) Mais especificamente, o título II da *Electronic Communications Privacy Act* ([194]) estabelece um sistema de direitos à privacidade e, como tal, rege o acesso das autoridades com funções coercivas ao conteúdo das comunicações por fios, orais e eletrónicas armazenadas por fornecedores terceiros de serviços ([195]). Criminaliza o acesso ilegal (ou seja, não autorizado pelo tribunal ou admissível de outro modo) a essas comunicações e prevê que uma pessoa afetada possa intentar uma ação cível num tribunal federal dos EUA para obter reparação por danos efetivos e punitivos, bem como uma compensação equitativa contra um funcionário do governo que tenha cometido intencionalmente esses atos ilegais, ou contra os Estados Unidos.

(133) Do mesmo modo, ao abrigo da *Freedom of Information Act* (FOIA, 5 U.S.C. § 552), qualquer pessoa tem o direito de obter acesso aos registos de uma agência federal e, após o esgotamento das soluções administrativas, de fazer valer esse direito em tribunal, exceto na medida em que esses registos sejam protegidos de divulgação pública por uma isenção ou uma exclusão especial decorrente do exercício de funções coercivas ([196]).

([191]) 5 U.S.C. § 702.

([192]) Geralmente, apenas as decisões «finais» de uma agência, e não as decisões «preliminares, processuais ou intermédias» de uma agência, estão sujeitas a um recurso judicial. Ver 5 U.S.C. § 704.

([193]) 5 U.S.C. § 706(2)(A).

([194]) 18 U.S.C. §§ 2701-2712.

([195]) O ECPA protege as comunicações detidas por dois tipos definidos de fornecedores de serviços de rede, nomeadamente os fornecedores de: i) serviços de comunicações eletrónicas, por exemplo telefonia ou correio eletrónico; ii) serviço informático à distância, como suportes informáticos ou serviços de processamento.

([196]) Estas exclusões são, contudo, enquadradas. Por exemplo, de acordo com o 5 U.S.C. § 552 (b)(7), os direitos atribuídos ao abrigo da FOIA são excluídos para os «documentos ou informações recolhidos para fins coercivos, mas apenas se a apresentação desses documentos ou as informações em matéria coerciva (A) puder razoavelmente ser considerada uma interferência na ação repressiva, (B) privasser uma pessoa de um direito a um processo equitativo ou a um julgamento imparcial, (C) puder razoavelmente ser considerada como constituindo uma invasão injustificada da vida privada, (D) puder razoavelmente ser considerada como divulgando a identidade de uma fonte confidencial, nomeadamente de uma agência ou de uma autoridade nacional, local ou estrangeira ou de qualquer instituição privada que tivesse fornecido informações a título confidencial e, no caso de um documento ou de informações recolhidas pelos serviços com funções coercivas no quadro de uma investigação penal ou por uma agência que procede a uma investigação nacional legal em matéria de informações de segurança, informações fornecidas por uma fonte confidencial, (E) tiver por efeito divulgar as técnicas e procedimentos das investigações e das ações penais, ou divulgar as orientações aplicadas às investigações e ações penais realizadas pelos serviços com funções repressivas, se se puder razoavelmente esperar que essa divulgação contornaria a lei, ou (F) se a divulgação da existência de tais documentos puder pôr em perigo a vida ou a segurança física de uma pessoa». Do mesmo modo, «quando qualquer pedido que implique o acesso a documentos [cuja apresentação poderia razoavelmente ser considerada um entrave a uma ação repressiva] e (A) a investigação ou o procedimento implicar uma eventual violação do direito penal; e (B) existam razões para crer que i) a pessoa objeto da investigação ou do procedimento não está consciente da respetiva existência, e ii) a divulgação da existência de documentos poderia razoavelmente ser considerada um entrave a uma ação repressiva, a agência pode, durante um período limitado ao período durante o qual esta circunstância continua a prevalecer, tratar os documentos como não estando sujeitos às disposições da presente secção.» (5 U.S.C. § 552 (c)(1)).

(134) Além disso, várias outras leis garantem às pessoas o direito de intentar um processo contra uma autoridade pública ou um funcionário americano no que diz respeito ao tratamento dos seus dados pessoais, tais como a *Wiretap Act* ([197]), a *Computer Fraud and Abuse Act* ([198]), a *Federal Torts Claim Act* ([199]), a *Right to Financial Privacy Act* ([200]), e a *Fair Credit Reporting Act* ([201]).

(135) Por conseguinte, a Comissão conclui que existem normas em vigor nos Estados Unidos destinadas a limitar qualquer ingerência, para efeitos do exercício de funções coercivas ([202]) ou outros efeitos de interesse público, nos direitos fundamentais das pessoas cujos dados pessoais são transferidos da União para os Estados Unidos ao abrigo do Escudo de Proteção da Privacidade UE-EUA ao estritamente necessário para a consecução do objetivo legítimo em questão e que asseguram a proteção jurídica eficaz contra tal ingerência.

4. NÍVEL DE PROTEÇÃO ADEQUADO AO ABRIGO DO ESCUDO DE PROTEÇÃO DA PRIVACIDADE UE-EUA

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

(137) Nomeadamente, a Comissão considera que, no seu conjunto, os princípios emitidos pelo *Department of Commerce* asseguram um nível de proteção dos dados pessoais que é essencialmente equivalente ao assegurado pelos princípios de base estabelecidos na Diretiva 95/46/CE.

(138) Além disso, a aplicação eficaz dos princípios é garantida pelas obrigações de transparência e pela administração do Escudo de Proteção da Privacidade pelo *Department of Commerce*.

(139) Além disso, a Comissão considera que, como um todo, os mecanismos de supervisão e recurso previstos pelo Escudo de Proteção permitem, na prática, a identificação e sanção das infrações aos princípios de privacidade por parte das organizações aderentes ao Escudo de Proteção da Privacidade e oferecem vias de recurso ao titular de dados que lhe dão acesso aos seus dados pessoais, permitindo a retificação ou eliminação de tais dados.

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

([197]) 18 U.S.C. §§ 2510 e seg. Ao abrigo da *Wiretap Act* (18 U.S.C. § 2520), uma pessoa cuja comunicação telefónica, verbal ou eletrónica é intercetada, divulgada ou deliberadamente utilizada pode intentar uma ação cível por violação da *Wiretap Act*, incluindo, em certas circunstâncias, contra um funcionário do governo ou contra os Estados Unidos. Para a recolha de informações relativas ao endereço e outras informações não referentes ao conteúdo (por exemplo, endereço IP, endereço eletrónico destinatário/emissor), ver igualmente o capítulo *Pen Registers and Trap and Trace Devices* do título 18 (18 U.S.C. §§ 3121-3127 e, para uma ação cível, § 2707).

([198]) 18 U.S.C. § 1030. Ao abrigo da *Computer Fraud and Abuse Act*, qualquer pessoa pode intentar uma ação contra qualquer pessoa por acesso não autorizado intencional (ou por ter excedido um acesso autorizado) a fim de obter informações junto de um estabelecimento financeiro, de um sistema informático das autoridades americanas ou de um outro sistema específico, incluindo, em certas circunstâncias, contra um funcionário do governo.

([199]) 28 U.S.C. §§ 2671 e seg. Ao abrigo da *Federal Tort Claims Act*, qualquer pessoa pode intentar uma ação, em certas circunstâncias, contra os Estados Unidos no que diz respeito a «atos ou omissões negligentes ou ilegítimas que comete qualquer funcionário do Estado agindo no quadro das suas funções ou do seu emprego.»

([200]) 12 U.S.C. §§ 3401 e seg. Ao abrigo da *Right to Financial Privacy Act*, qualquer pessoa pode intentar uma ação, em certas circunstâncias, contra os Estados Unidos por obtenção ou divulgação de documentos financeiros protegidos em violação da lei. O acesso do governo aos documentos financeiros protegidos é, em geral, proibido, a menos que o governo efetue o pedido mediante uma intimação legal ou um mandato de busca ou, sujeito a limitações, um pedido escrito oficial e que a pessoa, relativamente à qual são solicitadas informações, receba notificação do pedido.

([201]) 15 U.S.C. §§ 1681-1681x. Ao abrigo da *Fair Credit Reporting Act*, qualquer pessoa pode intentar uma ação contra qualquer pessoa que não cumpra os requisitos (nomeadamente a necessidade de uma autorização legal) no que se refere à recolha, divulgação e utilização de informações sobre os créditos ao consumo, ou, em certas circunstâncias, contra uma agência governamental.

([202]) O Tribunal de Justiça reconheceu que a aplicação da lei constitui um objetivo legítimo. Ver os processos apensos C-293/12 e C-594/12, *Digital Rights Ireland e outros*, EU:C:2014:238, n.º 42; Ver igualmente o artigo 8.º, n.º 2, TEDH e o acórdão proferido pelo Tribunal Europeu dos Direitos do Homem no processo *Weber e Saravia*/Alemanha, Queixa n.º 54934/00, n.º 104.

(141) A Comissão conclui que o que precede observa as normas do artigo 25.º da Diretiva 95/46/CE, interpretado à luz da Carta dos Direitos Fundamentais da União Europeia, tal como explicado pelo Tribunal de Justiça, nomeadamente no acórdão *Schrems*.

5. AÇÃO DAS AUTORIDADES RESPONSÁVEIS PELA PROTEÇÃO DOS DADOS E INFORMAÇÃO À COMISSÃO

(142) No acórdão *Schrems*, o Tribunal de Justiça esclareceu que a Comissão não tem competência para limitar os poderes das APD decorrentes do artigo 28.º da Diretiva 95/46/CE (nomeadamente o poder de suspensão de transferências de dados) sempre que uma pessoa, na apresentação de um pedido nos termos da referida disposição, questione a compatibilidade de uma decisão de adequação da Comissão com a proteção do direito fundamental à privacidade e à proteção dos dados ([203]).

(143) A fim de acompanhar eficazmente o funcionamento do Escudo de Proteção da Privacidade, a Comissão deve ser informada pelos Estados-Membros sobre as medidas relevantes tomadas pelas APD.

(144) Além disso, o Tribunal de Justiça considerou que, em conformidade com o artigo 25.º, n.º 6, segundo parágrafo, da Diretiva 95/46/CE, os Estados-Membros e os respetivos organismos devem tomar as medidas necessárias para dar cumprimento aos atos das instituições da União, uma vez que se presume que estes últimos são legais e, em conformidade, produzem efeitos legais até ao momento em que são revogados, anulados num recurso de anulação ou declarados inválidos na sequência de um pedido de decisão prejudicial ou uma exceção de ilegalidade. Consequentemente, uma decisão de adequação da Comissão adotada nos termos do artigo 25.º, n.º 6, da Diretiva 95/46/CE é vinculativa para todos os organismos dos Estados-Membros aos quais se destina, nomeadamente para as suas autoridades independentes de supervisão ([204]). Sempre que tal autoridade tenha recebido uma queixa que coloque em causa a conformidade de uma decisão de adequação da Comissão com a proteção do direito fundamental à privacidade e à proteção dos dados e considere que as objeções apresentadas são fundamentadas, a legislação nacional deve proporcionar-lhe uma via de recurso que lhe permite apresentar tais objeções perante um tribunal nacional que, em caso de dúvida, deve suspender a instância e efetuar um pedido de decisão prejudicial ao Tribunal de Justiça ([205]).

6. REAPRECIAÇÃO PERIÓDICA DA VERIFICAÇÃO DE ADEQUAÇÃO

(145) Tomando em consideração o facto de o nível de proteção conferido pela ordem jurídica dos EUA poder ser suscetível de alterações, a Comissão, na sequência da adoção da presente decisão, verificará periodicamente se as conclusões relativas à adequação do nível de proteção assegurado pelos Estados Unidos ao abrigo do Escudo de Proteção da Privacidade UE-EUA se mantêm factual e legalmente justificadas. De qualquer modo, tal verificação é necessária sempre que a Comissão obtenha informações que suscitem dúvidas justificadas a esse respeito ([206]).

(146) Portanto, a Comissão acompanhará continuamente o enquadramento global para a transferência de dados pessoais criado pelo Escudo de Proteção da Privacidade UE-EUA, bem como a observância pelas autoridades dos EUA das declarações e compromissos constantes dos documentos que figuram em anexo à presente decisão. Para facilitar este processo, os Estados Unidos comprometeram-se a informar a Comissão de qualquer evolução importante da legislação americana que apresente um interesse para o Escudo de Proteção da Privacidade no domínio da proteção dos dados pessoais e as limitações e garantias aplicáveis ao acesso das autoridades públicas aos dados pessoais. Além disso, a presente decisão será objeto de uma reapreciação conjunta anual que abrangerá todos os aspetos do funcionamento do Escudo de Proteção da Privacidade UE-EUA, nomeadamente a utilização das derrogações aos princípios relativas à segurança nacional e ao exercício de funções coercivas. Além disso, uma vez que a verificação de adequação poderia igualmente ser influenciada por evoluções jurídicas no direito da União, a Comissão avaliará o nível de proteção assegurado pelo Escudo de Proteção da Privacidade na sequência da entrada em vigor do Regulamento Geral sobre a Proteção de Dados.

(147) Para realizar a reapreciação conjunta anual a que se referem os anexos I, II e VI, a Comissão reunirá com o *Department of Commerce* e a FTC, acompanhados, se adequado, de outros departamentos e serviços envolvidos na aplicação das disposições do Escudo de Proteção da Privacidade, bem como, no que se refere a questões relativas à segurança nacional, representantes do ODNI, outros elementos do setor das informações e o Mediador. A participação nesta reunião será aberta às APD da UE e aos representantes do grupo de trabalho do artigo 29.º.

([203]) *Schrems*, n.ºs 40 e seguintes, 101-103.
([204]) *Schrems*, n.ºs 51, 52 e 62.
([205]) *Schrems*, n.º 65.
([206]) *Schrems*, n.º 76.

(148) No âmbito da reapreciação conjunta anual, a Comissão solicitará que o *Department of Commerce* apresente informações abrangentes sobre todos os aspetos relevantes do funcionamento do Escudo de Proteção da Privacidade UE-EUA, nomeadamente queixas submetidas ao *Department of Commerce* pelas APD e os resultados das verificações de conformidade oficiosas. A Comissão também solicitará esclarecimentos relativamente a quaisquer questões ou assuntos relativos ao Escudo de Proteção da Privacidade UE-EUA e ao seu funcionamento decorrentes das informações disponíveis, nomeadamente relatórios de transparência autorizados nos termos da *Freedom Act*, relatórios públicos elaborados pelos serviços de informações nacionais dos EUA, pelas APD, grupos de proteção da privacidade, relatórios dos meios de comunicação social ou outras fontes possíveis. Além disso, a fim de facilitar a tarefa da Comissão a este respeito, os Estados-Membros devem informar a Comissão dos casos em que as ações dos organismos responsáveis por assegurar a conformidade com os princípios nos EUA não asseguram essa conformidade, bem como de quaisquer indícios de que as ações das autoridades públicas dos EUA responsáveis pela segurança nacional ou pela prevenção, investigação, deteção ou repressão de infrações penais não asseguram o nível de proteção exigido.

(149) Com base na reapreciação conjunta anual, a Comissão preparará um relatório público a apresentar ao Parlamento Europeu e ao Conselho.

7. SUSPENSÃO DA DECISÃO DE ADEQUAÇÃO

(150) Sempre que, com base nas verificações ou em quaisquer outras informações disponíveis, a Comissão conclua que o nível de proteção assegurado pelo Escudo de Proteção da Privacidade já não pode ser considerado como fundamentalmente equivalente ao que é garantido na União ou que existem indícios claros de que a conformidade efetiva com os princípios nos Estados Unidos pode já não estar assegurada, ou que as ações das autoridades públicas dos EUA responsáveis pela segurança nacional ou pela prevenção, investigação, deteção ou repressão de infrações penais não asseguram o nível de proteção exigido, a Comissão informará o *Department of Commerce* deste facto e solicitará a tomada de medidas adequadas a fim de resolver rapidamente os potenciais incumprimentos dos princípios num prazo especificado e razoável. Se, após o termo do prazo especificado, as autoridades dos EUA não demonstrarem de modo satisfatório que o Escudo de Proteção da Privacidade UE-EUA continua a assegurar o cumprimento efetivo e um nível de proteção adequado, a Comissão dará início a um procedimento conducente à suspensão parcial ou total ou à revogação da presente decisão ([207]). Em alternativa, a Comissão pode propor a alteração da presente decisão, por exemplo, limitando o âmbito de aplicação da verificação de adequação apenas às transferências de dados sujeitas a condições adicionais.

(151) Em especial, a Comissão dará início ao procedimento de suspensão ou revogação em caso de:

a) informações de que as autoridades dos EUA não cumprem as declarações e os compromissos constantes dos documentos que figuram em anexo à presente decisão, nomeadamente no que diz respeito às condições e limitações aplicáveis ao acesso das autoridades públicas dos EUA, para efeitos do exercício de funções coercivas, segurança nacional e outros efeitos de interesse público, aos dados pessoais transferidos ao abrigo do Escudo de Proteção da Privacidade;

b) não resolução eficaz das queixas apresentadas pelos titulares de dados da UE; a este respeito, a Comissão tomará em consideração todas as circunstâncias que afetam a possibilidade de os titulares de dados da UE fazerem valer os seus direitos, incluindo, nomeadamente, o compromisso assumido voluntariamente pelas empresas autocertificadas dos EUA de cooperar com as APD e respeitar o seu aconselhamento; ou

c) não apresentação, por parte do Mediador para o Escudo de Proteção da Privacidade, de respostas adequadas e em tempo útil aos pedidos dos titulares de dados da UE.

(152) A Comissão também ponderará dar início ao procedimento conducente à alteração, suspensão ou revogação da presente decisão se, no contexto da reapreciação conjunta anual do funcionamento do Escudo de Proteção da Privacidade UE-EUA ou de outro modo, o *Department of Commerce* ou outros departamentos ou serviços envolvidos na implementação do Escudo de Proteção da Privacidade, ou, no que se refere a questões relacionadas com segurança nacional, os representantes do setor das informações dos EUA ou o Mediador, não apresentarem as informações ou os esclarecimentos necessários para a verificação de conformidade com os princípios, da

([207]) A partir da data de aplicação do Regulamento Geral sobre a Proteção de Dados, a Comissão utilizará os seus poderes para adotar, por imperativos de urgência devidamente justificados, um ato de execução de suspensão da presente decisão, que será aplicável imediatamente sem a sua apresentação prévia ao respetivo comité de comitologia e permanecerá em vigor durante um período máximo de seis meses.

eficácia dos procedimentos para a resolução de queixas ou qualquer redução do nível de proteção exigido em consequência de ações dos serviços de informações nacionais dos EUA, designadamente na sequência da recolha e/ou do acesso a dados pessoais que não se limitem ao estritamente necessário e proporcionado. A este respeito, a Comissão tomará em consideração em que medida as informações relevantes podem ser obtidas a partir de outras fontes, nomeadamente através de relatórios de empresas autocertificadas dos EUA, conforme permitido nos termos da *Freedom Act*.

(153) O grupo de trabalho relativo à proteção das pessoas no que diz respeito ao tratamento de dados pessoais criado ao abrigo do artigo 29.º da Diretiva 95/46/CE publicou o seu parecer sobre o nível de proteção assegurado pelo Escudo de Proteção da Privacidade UE-EUA ([208]), que foi tomado em consideração na elaboração da presente decisão.

(154) O Parlamento Europeu adotou uma resolução sobre os fluxos de dados transatlânticos ([209]).

(155) As medidas previstas na presente decisão são conformes com o parecer do comité instituído pelo artigo 31.º, n.º 1, da Diretiva 95/46/CE,

ADOTOU A PRESENTE DECISÃO:

Artigo 1.º

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

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

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

Artigo 2.º

A presente decisão não afeta a aplicação das disposições da Diretiva 95/46/CE para além do artigo 25.º, n.º 1, relativamente ao tratamento de dados pessoais nos Estados-Membros, em especial, o artigo 4.º.

Artigo 3.º

Sempre que as autoridades competentes dos Estados-Membros exerçam os seus poderes nos termos do artigo 28.º, n.º 3, da Diretiva 95/46/CE conducentes à suspensão ou proibição definitiva de fluxos de dados para uma organização nos Estados Unidos que conste da lista do Escudo de Proteção da Privacidade em conformidade com as secções I e III dos princípios estabelecidos no anexo II a fim de proteger pessoas singulares no que diz respeito ao tratamento dos seus dados pessoais, o Estado-Membro em causa informa a Comissão sem demora.

Artigo 4.º

1. A Comissão acompanhará continuamente o funcionamento do Escudo de Proteção da Privacidade UE-EUA com vista a avaliar se os Estados Unidos continuam a assegurar um nível de proteção adequado dos dados pessoais transferidos nesse âmbito da União para organizações nos Estados Unidos.

([208]) Parecer 01/2016 sobre o projeto de decisão relativa ao nível de proteção assegurado pelo Escudo de Proteção da Privacidade UE-EUA, adotado em 13 de abril de 2016.
([209]) Resolução do Parlamento Europeu de 26 de maio de 2016 sobre os fluxos de dados transatlânticos [(2016/2727(RSP)].

2. Os Estados-Membros e a Comissão informam-se mutuamente de casos nos quais se afigure que os organismos governamentais dos Estados Unidos com poder legal para fazer cumprir os princípios estabelecidos no anexo II não fornecem mecanismos de deteção e supervisão eficazes que permitam, na prática, a identificação e sanção de infrações aos princípios.

3. Os Estados-Membros e a Comissão informam-se mutuamente sobre quaisquer informações de que as ingerências pelas autoridades públicas dos EUA, responsáveis pela segurança nacional, o exercício de funções coercivas ou outros interesses públicos, no direito das pessoas à proteção dos seus dados pessoais vão além do estritamente necessário e/ou de que não existe proteção jurídica eficaz contra tais ingerências.

4. No prazo de um ano a contar da data de notificação da presente decisão aos Estados-Membros e subsequentemente numa base anual, a Comissão avalia a aplicação constante do artigo 1.º, n.º 1, com base em todas as informações disponíveis, designadamente as informações recebidas como parte da reapreciação conjunta anual a que se referem os anexos I, II e VI.

5. A Comissão comunica todas as conclusões pertinentes ao comité instituído ao abrigo do artigo 31.º da Diretiva 95/46/CE.

6. A Comissão apresentará um projeto de medidas em conformidade com o procedimento a que se refere o artigo 31.º, n.º 2, da Diretiva 95/46/CE, com vista a suspender, alterar ou revogar a presente decisão ou a limitar o seu âmbito de aplicação, entre outros, sempre que haja informações:

— de que as autoridades públicas dos EUA não cumprem as declarações e os compromissos constantes dos documentos que figuram em anexo à presente decisão, nomeadamente no que diz respeito às condições e limitações aplicáveis ao acesso pelas autoridades públicas dos EUA com funções coercivas, responsáveis pela segurança nacional e outros interesses públicos aos dados pessoais transferidos ao abrigo do Escudo de Proteção da Privacidade UE-EUA;

— da não resolução sistemática das queixas apresentadas pelos titulares de dados da UE; ou

— da não apresentação sistemática, por parte do Mediador para o Escudo de Proteção da Privacidade, de respostas adequadas e em tempo útil aos pedidos dos titulares de dados da UE tal como previsto no anexo III, secção 4, alínea e).

A Comissão apresentará igualmente o referido projeto de medidas se a falta de cooperação dos organismos envolvidos na garantia do funcionamento do Escudo de Proteção da Privacidade UE-EUA nos Estados Unidos impedir a Comissão de verificar a aplicação do artigo 1.º, n.º 1.

Artigo 5.º

Os Estados-Membros tomarão todas as medidas necessárias para dar cumprimento à presente decisão.

Artigo 6.º

Os destinatários da presente decisão são os Estados-Membros.

Feito em Bruxelas, em 12 de julho de 2016.

Pela Comissão
Věra JOUROVÁ
Membro da Comissão

ANEXO I

Carta da Secretária do Comércio dos EUA, Penny Pritzker

7 de julho de 2016

Věra Jourová
Comissária da UE responsável pela Justiça, Consumidores e Igualdade de Género
Comissão Europeia
Rue de la Loi/Westraat 200
1049 Bruxelas
Bélgica

Excelentíssima Senhora Comissária Jourová:

Em nome dos Estados Unidos, tenho o prazer de transmitir um pacote de materiais relativos ao Escudo de Proteção da Privacidade UE-EUA que resulta de dois anos de debates produtivos entre as nossas equipas. Este pacote, a par de outros materiais acessíveis à Comissão a partir de fontes públicas, constitui uma base muito sólida para uma nova verificação de adequação por parte da Comissão Europeia ([1]).

Ambos devemos estar orgulhosos das melhorias efetuadas ao quadro. O Escudo de Proteção da Privacidade baseia-se em princípios que apresentam um forte apoio consensual em ambos os lados do Atlântico e reforçámos o seu funcionamento. Através do nosso trabalho conjunto, temos a possibilidade real de melhorar a proteção da privacidade em todo o mundo.

O pacote do Escudo de Proteção da Privacidade inclui os princípios do Escudo de Proteção da Privacidade, a par de uma carta, que figura no anexo 1, da *International Trade Administration* (ITA) do *Department of Commerce*, responsável pela administração do programa, que descreve os compromissos que o *Department of Commerce* assumiu a fim de assegurar o funcionamento eficaz do Escudo de Proteção da Privacidade. O pacote também inclui o anexo 2, que apresenta outros compromissos do *Department of Commerce* relacionados com o novo modelo de arbitragem disponível ao abrigo do Escudo de Proteção da Privacidade.

Incumbi o meu pessoal de envidar todos os recursos necessários para a aplicação do quadro do Escudo de Proteção da Privacidade de forma célere e integral e para assegurar o cumprimento dos compromissos assumidos nos anexos 1 e 2 em tempo útil.

O pacote do Escudo de Proteção da Privacidade inclui igualmente documentos de outros serviços dos Estados Unidos, nomeadamente:

— Uma carta da *Federal Trade Commission* (FTC) que descreve a sua aplicação do Escudo de Proteção da Privacidade;

— Uma carta do *Department of Transportation* que descreve a sua aplicação do Escudo de Proteção da Privacidade;

— Duas cartas elaboradas pelo *Office of the Director of National Intelligence* (Gabinete do Diretor dos Serviços Nacionais de Informações — ODNI) relativas às garantias e limitações aplicáveis aos serviços de segurança nacional dos EUA;

— Uma carta do *Department of State* e o memorando que a acompanha, que descrevem o compromisso do *State Department* de instituir um novo Mediador para o Escudo de Proteção da Privacidade para efeitos de apresentação de questões sobre as práticas dos Estados Unidos de recolha de informação de origem eletromagnética; e

— Uma carta elaborada pelo *Department of Justice* sobre as garantias e limitações do acesso do governo dos EUA para efeitos do exercício de funções coercivas e de interesse público.

Pode ter a certeza de que os Estados Unidos da América encaram estes compromissos com seriedade.

([1]) Uma vez que a Decisão da Comissão sobre a adequação da proteção assegurada pelo Escudo de Proteção da Privacidade UE-EUA é aplicável à Islândia, ao Liechtenstein e à Noruega, o pacote do Escudo de Proteção da Privacidade abrangerá tanto a União Europeia como estes três países.

No prazo de 30 dias a contar da aprovação final da decisão de adequação, todo o pacote do Escudo de Proteção da Privacidade será transmitido ao *Federal Register* para publicação.

Aguardamos com expectativa a possibilidade de trabalhar convosco na implementação do Escudo de Proteção da Privacidade e no início da próxima fase deste projeto em conjunto.

Queira aceitar a expressão da minha mais elevada consideração,

Penny Pritzker

Anexo 1

Carta do Subsecretário interino para as questões do comércio internacional, Ken Hyatt

Excelentíssima Senhora Věra Jourová
Comissária para a Justiça, Consumidores e Igualdade de Género
Comissão Europeia
Rue de la Loi/Westraat 200
1049 Bruxelas
Bélgica

Excelentíssima Senhora Comissária Jourová:

Em nome da *International Trade Administration*, tenho o prazer de descrever a melhoria da proteção dos dados pessoais que o quadro do Escudo de Proteção da Privacidade UE-EUA («Escudo de Proteção da Privacidade» ou «quadro») proporciona, bem como os compromissos que o *Department of Commerce* assumiu a fim de assegurar o funcionamento eficaz do Escudo de Proteção da Privacidade. A finalização deste acordo histórico constitui uma grande realização para a proteção da privacidade e as empresas em ambos os lados do Atlântico. Garante aos cidadãos da UE que os seus dados serão protegidos e que disporão de vias de recurso para resolver quaisquer preocupações. Proporciona a certeza de que contribuirá para o crescimento da economia transatlântica mediante a garantia de que milhares de empresas europeias e norte-americanas podem continuar a investir e a desenvolver a sua atividade através das nossas fronteiras. O Escudo de Proteção da Privacidade resulta de mais de dois anos de trabalho árduo e colaboração convosco, os nossos colegas da Comissão Europeia («Comissão»). Aguardamos com expectativa a continuação do trabalho com a Comissão a fim de assegurar que o Escudo de Proteção da Privacidade funciona como pretendido.

Temos vindo a colaborar com a Comissão no desenvolvimento do Escudo de Proteção da Privacidade para permitir que as organizações estabelecidas nos Estados Unidos cumpram os requisitos de adequação em matéria de proteção dos dados ao abrigo do direito da UE. O novo quadro produzirá vários benefícios significativos tanto para as pessoas singulares como para as empresas. Em primeiro lugar, proporciona um conjunto importante de proteções da privacidade no que se refere aos dados dos cidadãos da UE. Exige que as organizações participantes dos EUA desenvolvam uma política em matéria de proteção da privacidade conforme, que assumam publicamente o compromisso de cumprir os princípios do Escudo de Proteção da Privacidade para que este compromisso se torne executório nos termos do direito dos EUA, que renovem anualmente a certificação de conformidade ao *Department of Commerce*, que disponibilizem a resolução independente de litígios gratuita aos cidadãos da UE e que estejam sujeitas à autoridade da *Federal Trade Commission* («FTC»), do *Department of Transportation* («DOT») ou de qualquer outro organismo de execução. Em segundo lugar, o Escudo de Proteção da Privacidade permitirá que milhares de empresas nos Estados Unidos e filiais de empresas europeias nos Estados Unidos recebam dados pessoais da União Europeia com vista a facilitar os fluxos de dados subjacentes ao comércio transatlântico. A relação económica transatlântica já é a maior do mundo, representando metade da produção económica global e quase um bilião de USD no comércio de bens e serviços, apoiando milhões de empregos em ambos os lados do Atlântico. As empresas que dependem dos fluxos de dados transatlânticos de todos os setores industriais incluem grandes empresas que constam da lista «Fortune 500», bem como muitas pequenas e médias empresas (PME). Os fluxos de dados transatlânticos permitem que as organizações dos EUA procedam ao tratamento de dados necessários para oferecer bens, serviços e oportunidades de emprego aos cidadãos europeus. O Escudo de Proteção da Privacidade apoia princípios de privacidade partilhados, colmatando as diferenças nas nossas abordagens jurídicas, fazendo progredir ao mesmo tempo os objetivos comerciais e económicos da Europa e dos Estados Unidos.

Embora a decisão de uma empresa de aderir a este novo quadro seja voluntária, quando uma empresa adere publicamente ao Escudo de Proteção da Privacidade, o seu compromisso é executório nos termos do direito dos EUA, pela *Federal Trade Commission* ou pelo *Department of Transportation*, em função da autoridade competente no que diz respeito à organização aderente ao Escudo de Proteção da Privacidade.

Melhorias ao abrigo dos princípios do Escudo de Proteção da Privacidade

O Escudo de Proteção da Privacidade resultante reforça a proteção da privacidade da seguinte forma:

— exige que sejam fornecidas informações adicionais às pessoas no âmbito do princípio de aviso, nomeadamente uma declaração da participação da organização no Escudo de Proteção da Privacidade, uma declaração do direito de acesso da pessoa aos dados pessoais e a identificação do organismo independente de resolução de litígios relevante;

— reforça a proteção dos dados pessoais que são transferidos de uma organização aderente ao Escudo de Proteção da Privacidade para um terceiro responsável pelo tratamento dos dados, exigindo que as partes celebrem um contrato que preveja que tais dados podem ser tratados apenas para fins limitados e especificados em consonância com o consentimento dado pela pessoa e que o destinatário assegurará o mesmo nível de proteção que os princípios;

— reforça a proteção dos dados pessoais que são transferidos de uma organização aderente ao Escudo de Proteção da Privacidade para um terceiro agente, nomeadamente exigindo que a organização aderente ao Escudo de Proteção da Privacidade: tome medidas razoáveis e adequadas para garantir que o agente trata de modo eficaz as informações pessoais transferidas de forma coerente com as obrigações da organização nos termos dos princípios; após aviso, tome medidas razoáveis e adequadas para cessar e corrigir o tratamento não autorizado; e apresente ao *Department of Commerce*, mediante pedido, um resumo ou uma cópia representativa das disposições relevantes em matéria de proteção da privacidade do seu contrato com esse agente;

— assegura que a organização aderente ao Escudo de Proteção da Privacidade é responsável pelo tratamento das informações pessoais que recebe ao abrigo do Escudo de Proteção da Privacidade e subsequentemente transfere para um terceiro que desempenha a função de agente em seu nome, e que a organização aderente ao Escudo de Proteção da Privacidade permanece responsável nos termos dos princípios se o seu agente proceder ao tratamento dessas informações pessoais de forma incoerente com os princípios, a menos que a organização prove que não é responsável pela situação conducente aos danos;

— esclarece que as organizações do Escudo de Proteção da Privacidade devem limitar as informações pessoais às informações relevantes para as finalidades do tratamento;

— exige que as organizações certifiquem anualmente junto do *Department of Commerce* o seu compromisso de aplicar os princípios às informações que receberam durante a sua participação no Escudo de Proteção da Privacidade se o abandonaram e optaram por conservar os referidos dados;

— exige que sejam disponibilizados mecanismos de recurso independentes sem custos para a pessoa em causa;

— exige que as organizações e os respetivos mecanismos de recurso independentes selecionados respondam imediatamente às questões e aos pedidos de informações apresentados pelo *Department of Commerce* sobre o Escudo de Proteção da Privacidade;

— exige que as organizações respondam com celeridade às queixas relativas à conformidade com os princípios submetidas pelas autoridades dos Estados-Membros da UE através do *Department of Commerce*; e

— exige que as organizações do Escudo de Proteção da Privacidade publiquem todas as secções relevantes relacionadas com o Escudo de Proteção da Privacidade dos relatórios de conformidade ou avaliação apresentados à FTC, caso sejam objeto de uma decisão judicial ou da FTC com base numa situação de incumprimento.

Administração e supervisão do programa do Escudo de Proteção da Privacidade pelo *Department of Commerce*

O *Department of Commerce* reitera o seu compromisso de manter e disponibilizar ao público uma lista oficial de organizações dos EUA que declararam a sua adesão ao *Department of Commerce*, bem como o seu compromisso de aderir aos princípios («a lista do Escudo de Proteção da Privacidade»). O *Department of Commerce* manterá a lista do Escudo de Proteção da Privacidade atualizada através da supressão das organizações que abandonem o programa voluntariamente, não efetuem a renovação da certificação anual em conformidade com os procedimentos do *Department of Commerce* ou não cumpram persistentemente os princípios. O *Department of Commerce* também manterá e disponibilizará ao público um registo oficial das organizações dos EUA que declararam previamente a sua adesão ao *Department of Commerce*, mas que foram suprimidas da lista do Escudo de Proteção da Privacidade, nomeadamente das que foram suprimidas devido ao incumprimento persistente dos princípios. O *Department of Commerce* identificará o motivo pelo qual cada organização foi suprimida.

Além disso, o *Department of Commerce* compromete-se a reforçar a administração e supervisão do Escudo de Proteção da Privacidade. Mais especificamente, o *Department of Commerce* tomará as seguintes medidas:

Apresentará informações adicionais no sítio Web do Escudo de Proteção da Privacidade

— manterá a lista do Escudo de Proteção da Privacidade, bem como um registo das organizações que declararam previamente a sua adesão aos princípios, mas que já não beneficiam do Escudo de Proteção da Privacidade;

— apresentará uma explicação num local de destaque, esclarecendo que todas as organizações suprimidas da lista do Escudo de Proteção da Privacidade já não beneficiam do mesmo, mas que, todavia, devem continuar a aplicar os princípios às informações pessoais que receberam durante a sua participação no Escudo de Proteção da Privacidade enquanto conservarem tais informações; e

— fornecerá uma ligação para os casos da FTC relacionados com o Escudo de Proteção da Privacidade apresentados no sítio Web da FTC.

Verificará os requisitos de autocertificação

— antes da conclusão da autocertificação de uma organização (ou da renovação anual) e da inclusão da organização na lista do Escudo de Proteção da Privacidade, verificará que esta última tomou as seguintes medidas:

  — apresentou as informações de contacto necessárias da organização;

  — descreveu as atividades da organização em matéria de informação pessoal recebida da UE;

  — indicou as informações pessoais abrangidas pela sua autocertificação;

  — se a organização dispuser de um sítio Web público, apresentou o endereço Web onde a política em matéria de proteção da privacidade se encontra disponível e esta encontra-se acessível no endereço Web fornecido ou, se uma organização não dispuser de um sítio Web público, indicou o local onde o público pode consultar a política em matéria de proteção da privacidade;

  — incluiu, na sua política relevante em matéria de proteção da privacidade, uma declaração que atesta que adere aos princípios e se a referida política se encontrar disponível em linha, uma hiperligação para o sítio Web do *Department of Commerce* relativo ao Escudo de Proteção da Privacidade;

  — identificou os organismos oficiais concretos com competência para deliberar sobre quaisquer queixas contra a organização em matéria de possíveis práticas desleais ou desonestas e violações das leis ou normas que regulamentam a proteção da vida privada (e que se encontram referidos nos princípios ou num futuro anexo dos princípios);

  — se a organização optar por satisfazer os requisitos estabelecidos na alínea a), subalíneas i) e iii), do princípio de recurso, aplicação e responsabilidade, comprometendo-se a cooperar com as autoridades adequadas da UE responsáveis pela proteção dos dados («APD»), indicou a sua intenção de cooperar com as APD na investigação e resolução de queixas apresentadas no âmbito do Escudo de Proteção da Privacidade, nomeadamente para responder às suas questões sempre os titulares de dados da UE tenham apresentado queixas diretamente às suas APD nacionais;

  — identificou qualquer programa relativo à proteção da vida privada em que a organização participe;

  — identificou o método de verificação para assegurar o respeito dos princípios (por exemplo, interno ou por terceiros);

  — identificou, tanto na sua declaração de autocertificação como na sua política em matéria de proteção da privacidade, o mecanismo de recurso independente que pode ser utilizado para investigar as queixas por resolver;

  — incluiu na sua política relevante em matéria de proteção da privacidade, se a política se encontrar disponível em linha, uma hiperligação para o sítio Web ou um formulário de apresentação de queixas do mecanismo de recurso independente que pode ser utilizado para investigar queixas por resolver; e

  — se a organização tiver indicado que tenciona receber informações relativas a recursos humanos transferidas da UE para utilização no contexto da relação laboral, declarou o seu compromisso de cooperar e respeitar as APD a fim de resolver queixas relativas às suas atividades no que se refere a tais dados, apresentou uma cópia da sua política em matéria de proteção da privacidade dos seus recursos humanos ao *Department of Commerce* e indicou onde a referida política se encontra disponível para consulta pelos seus funcionários em causa.

— colaborará com mecanismos de recurso independentes para verificar que as organizações se registaram efetivamente junto do mecanismo relevante indicado nas suas declarações de autocertificação, sempre que tal registo seja exigido.

Ampliará esforços para acompanhar as organizações que tenham sido suprimidas da lista do Escudo de Proteção da Privacidade

— notificará as organizações que são suprimidas da lista do Escudo de Proteção da Privacidade por «incumprimento persistente» de que não têm direito a preservar as informações recolhidas ao abrigo do Escudo de Proteção da Privacidade; e

— enviará questionários às organizações cujas autocertificações tenham caducado ou que tenham abandonado voluntariamente o Escudo de Proteção da Privacidade a fim de verificar se a organização devolverá, eliminará ou continuará a aplicar os princípios às informações pessoais que receberam enquanto participavam no Escudo de Proteção da Privacidade e, caso as informações pessoais sejam conservadas, verificará quem, no seio da organização, será o ponto de contacto permanente para o esclarecimento de questões relacionadas com o Escudo de Proteção da Privacidade.

Pesquisará e resolverá falsas alegações de participação

— reverá as políticas em matéria de proteção da privacidade das organizações que tenham participado previamente no programa do Escudo de Proteção da Privacidade, mas que tenham sido suprimidas da respetiva lista com o intuito de identificar possíveis falsas alegações de participação no programa;

— numa base contínua, sempre que uma organização: a) deixe de participar no Escudo de Proteção da Privacidade, b) não renove a certificação da sua adesão aos princípios ou c) seja excluída como participante no Escudo de Proteção da Privacidade, designadamente devido a «incumprimento persistente», verificará, sistematicamente, se a organização suprimiu da política relevante em matéria de proteção da privacidade todas as referências ao Escudo de Proteção da Privacidade que sugerem que a organização continua a participar ativamente no referido programa e tem direito aos seus benefícios. Sempre que o *Department of Commerce* conclua que tais referências não foram suprimidas, esta entidade avisará a organização de que, conforme adequado, submeterá esta questão ao organismo relevante para possíveis medidas de execução se a organização continuar a alegar a sua adesão ao Escudo de Proteção da Privacidade. Se a organização não suprimir as referências nem autocertificar a sua adesão ao Escudo de Proteção da Privacidade, o *Department of Commerce* submeterá sistematicamente a questão à FTC, ao DOT ou a outro organismo de execução adequado, podendo também, em casos adequados, tomar medidas para aplicar a marca de certificação do Escudo de Proteção da Privacidade;

— envidará outros esforços para identificar falsas alegações de participação no Escudo de Proteção da Privacidade e a utilização indevida da respetiva marca de certificação, nomeadamente através da realização de pesquisas na Internet a fim de identificar onde são exibidas imagens da marca de certificação do Escudo de Proteção da Privacidade, bem como referências ao quadro nas políticas em matéria de proteção da privacidade das organizações;

— resolverá de imediato todos os problemas identificados durante o acompanhamento sistemático de falsas alegações de participação e utilização indevida da marca de certificação, nomeadamente através do aviso às organizações que alegam falsamente a sua participação no Escudo de Proteção da Privacidade, tal como descrito acima;

— tomará outras medidas corretivas adequadas, designadamente o prosseguimento de todas as vias de recurso à disposição do *Department of Commerce* e a transmissão da questão à FTC, ao DOT, ou a outro organismo de execução adequado; e

— reexaminará e resolverá prontamente as queixas relativas a falsas alegações de participação recebidas.

O *Department of Commerce* procederá à reapreciação das políticas em matéria de proteção da privacidade das organizações a fim de identificar e resolver com maior eficácia as falsas alegações de participação no Escudo de Proteção da Privacidade. Especificamente, o *Department of Commerce* procederá à reapreciação das políticas em matéria de proteção da privacidade das organizações cuja autocertificação tenha caducado devido ao facto de não terem renovado a certificação da sua adesão aos princípios. O *Department of Commerce* realizará este tipo de reapreciação para verificar se as organizações suprimiram das políticas públicas relevantes em matéria de proteção da privacidade todas as referências que sugerem que as organizações continuam a participar ativamente no Escudo de Proteção da Privacidade. Em consequência destes tipos de reapreciações, identificaremos as organizações que não suprimiram tais referências e enviar-lhes-emos uma carta do *Office of General Counsel* do *Department of Commerce* com um aviso relativo a potenciais medidas de execução se as referências não forem eliminadas. O *Department of Commerce* tomará medidas de acompanhamento para garantir que a organização suprime as referências inadequadas ou renova a certificação da sua adesão aos princípios. Além disso, o *Department of Commerce* envidará esforços para identificar falsas alegações de participação no Escudo de Proteção da Privacidade efetuadas por organizações que nunca participaram no programa e tomará medidas corretivas semelhantes no que se refere a tais organizações.

Realizará verificações de conformidade sistemáticas, bem como avaliações do programa

— numa base contínua, controlará o cumprimento efetivo, nomeadamente através do envio de questionários pormenorizados às organizações participantes, a fim de identificar questões que careçam de acompanhamento posterior. Nomeadamente, tais verificações de conformidade devem ocorrer sempre que: a) o *Department of Commerce* tenha recebido queixas válidas específicas sobre a conformidade da organização com os princípios, b) uma organização não responda de forma válida aos pedidos de informações apresentados pelo *Department of Commerce* sobre o Escudo de Proteção da Privacidade, ou c) existam provas credíveis de que uma organização não cumpre os seus compromissos ao abrigo do Escudo de Proteção da Privacidade. Sempre que adequado, o *Department of Commerce* consultará as autoridades competentes em matéria de proteção dos dados sobre tais verificações de conformidade; e

— avaliará periodicamente a administração e a supervisão do programa do Escudo de Proteção da Privacidade a fim de assegurar que os esforços de acompanhamento são adequados para resolver novos problemas à medida que estes surjam.

O *Department of Commerce* aumentou os recursos que serão dedicados à administração e supervisão do programa do Escudo de Proteção da Privacidade, designadamente a duplicação do número de funcionários responsáveis pela administração e supervisão do programa. Continuaremos a dedicar recursos adequados a estes esforços a fim de assegurar o acompanhamento e a administração eficazes do programa.

Adaptará o sítio Web do Escudo de Proteção da Privacidade a públicos específicos

O *Department of Commerce* adaptará o sítio Web do Escudo de Proteção da Privacidade para incidir sobre três públicos-alvo: cidadãos da UE, empresas da UE e empresas dos EUA. A inclusão de material destinado diretamente aos cidadãos da UE e às empresas da UE facilitará a transparência de várias formas. No que se refere aos cidadãos da UE, explicará claramente: 1) os direitos que o Escudo de Proteção da Privacidade confere aos cidadãos da UE; 2) os mecanismos de recurso acessíveis aos cidadãos da UE sempre que estes considerem que uma organização infringiu o seu compromisso de respeitar os princípios; e 3) como encontrar informações relativas à autocertificação de adesão de uma organização ao Escudo de Proteção da Privacidade. No respeitante às empresas da UE, facilitará a verificação dos seguintes elementos: 1) se uma organização beneficia do Escudo de Proteção da Privacidade; 2) o tipo de informações abrangidas pela autocertificação de adesão de uma organização ao Escudo de Proteção da Privacidade; 3) a política em matéria de proteção da privacidade aplicável às informações abrangidas; e 4) o método utilizado pela organização para verificar a sua adesão aos princípios.

Aumentará a cooperação com as APD

Para aumentar as oportunidades de cooperação com as APD, o *Department of Commerce* criará um contacto dedicado que estabelecerá contactos com as APD. Nos casos em que a APD considere que uma organização não cumpre os princípios, designadamente na sequência de uma queixa de um cidadão da UE, a APD pode contactar o contacto dedicado do *Department of Commerce* para solicitar uma reapreciação mais pormenorizada da organização. Serão igualmente submetidas ao contacto queixas relativas às organizações que alegam falsamente participar no Escudo de Proteção da Privacidade, não obstante o facto de nunca terem autocertificado a sua adesão aos princípios. O contacto assistirá as APD na pesquisa de informações relacionadas com a autocertificação de uma organização específica ou com a anterior participação no programa e o contacto responderá às questões da APD sobre a aplicação de requisitos específicos do Escudo de Proteção da Privacidade. Em segundo lugar, o *Department of Commerce* fornecerá às APD o material relativo ao Escudo de Proteção da Privacidade para inclusão nos próprios sítios Web a fim de aumentar a transparência para os cidadãos e empresas da UE. O aumento da sensibilização relativamente ao Escudo de Proteção da Privacidade e às responsabilidades que este cria deve facilitar a identificação de problemas à medida que estes surgem, de modo a resolvê-los de forma adequada.

Facilitará a resolução de queixas de incumprimento

O *Department of Commerce*, através do contacto dedicado, receberá queixas submetidas por uma APD de que uma organização aderente ao Escudo de Proteção da Privacidade não cumpre os princípios. O *Department of Commerce* envidará os seus melhores esforços para facilitar a resolução da queixa junto da organização aderente ao Escudo de Proteção da Privacidade. No prazo de 90 dias após a receção da queixa, o *Department of Commerce* apresentará uma atualização à APD. A fim de facilitar a apresentação destas queixas, o *Department of Commerce* criará um formulário normalizado que as APD apresentarão junto do contacto dedicado do *Department of Commerce*. O contacto dedicado acompanhará todas as queixas submetidas pelas APD ao *Department of Commerce* e este último apresentará, na reapreciação anual descrita abaixo, um relatório de análise agregada das queixas que recebe todos os anos.

Adotará procedimentos de arbitragem e selecionará árbitros em consulta com a Comissão

O *Department of Commerce* cumprirá os seus compromissos nos termos do anexo I e publicará os procedimentos depois de se ter alcançado um acordo.

Mecanismo de reapreciação conjunta do funcionamento do Escudo de Proteção da Privacidade

O *Department of Commerce*, a FTC, e outros organismos, conforme adequado, realizarão reuniões anuais com a Comissão, as APD interessadas e representantes adequados do grupo de trabalho do artigo 29.º, nas quais o *Department of Commerce* apresentará informações atualizadas sobre o programa do Escudo de Proteção da Privacidade. As reuniões anuais incluirão a discussão de questões atuais relacionadas com o funcionamento, a aplicação, a supervisão e a execução do Escudo de Proteção da Privacidade, nomeadamente as queixas submetidas pelas APD ao *Department of Commerce*, os resultados de verificações oficiosas de conformidade e também podem incluir debates sobre alterações relevantes à legislação. Consoante o caso, a primeira reapreciação anual e reapreciações posteriores incluirão um diálogo sobre outros temas, tais como a tomada de decisões automatizadas, incluindo aspetos relacionados com as diferenças e semelhanças das abordagens da UE e dos EUA.

Atualização da legislação

O *Department of Commerce* deve efetuar todas as diligências razoáveis para informar a Comissão dos desenvolvimentos significativos da legislação nos Estados Unidos, desde que sejam pertinentes para o Escudo de Proteção da Privacidade em matéria de proteção de dados, e das limitações e salvaguardas aplicáveis ao acesso a dados pessoais por parte das autoridades dos EUA e sua subsequente utilização.

Derrogação por motivos de segurança nacional

No que se refere às limitações à adesão aos princípios do Escudo de Proteção da Privacidade para efeitos de segurança nacional, o Conselheiro-Geral do *Office of the Director of National Intelligence*, Robert Litt, também enviou duas cartas destinadas a Justin Antonipillai e Ted Dean do *Department of Commerce*, e estas foram-lhe transmitidas. Estas cartas discutem em pormenor, entre outras questões, as políticas, garantias e limitações aplicáveis às atividades de informação de origem eletromagnética realizadas pelos EUA. Além disso, descrevem a transparência proporcionada pelo setor das informações no que se refere a estas questões. Uma vez que a Comissão se encontra a avaliar o quadro do Escudo de Proteção da Privacidade, as informações apresentadas nestas cartas oferecem garantias que permitem concluir que o referido quadro funcionará de modo adequado, em conformidade com os seus princípios. Compreendemos que, no futuro, possa obter informações divulgadas ao público pelo setor das informações, a par de outras informações, que serão integradas na reapreciação anual do quadro do Escudo de Proteção da Privacidade.

Com base nos princípios do Escudo de Proteção da Privacidade e nas cartas e nos materiais que os acompanham, nomeadamente os compromissos do *Department of Commerce* relativamente à administração e supervisão do quadro do Escudo de Proteção da Privacidade, a nossa expectativa é de que a Comissão determinará que o quadro do Escudo de Proteção da Privacidade UE-EUA proporciona um nível de proteção adequado para efeitos do direito da UE e que as transferências de dados da União Europeia continuarão para as organizações que participam no Escudo de Proteção da Privacidade.

Queira aceitar a expressão da minha mais elevada consideração,

Ken Hyatt

Anexo 2

Modelo de arbitragem

ANEXO I

O presente anexo I apresenta as condições segundo as quais as organizações aderentes ao Escudo de Proteção da Privacidade são obrigadas a proceder à arbitragem de queixas, nos termos do princípio de recurso, aplicação e responsabilidade. A opção de arbitragem vinculativa descrita abaixo é aplicável a determinadas queixas «não resolvidas» relativas aos dados abrangidos pelo Escudo de Proteção da Privacidade UE-EUA. O objetivo desta opção consiste em oferecer um mecanismo célere, independente e equitativo, à escolha dos cidadãos, para a resolução de alegadas violações dos princípios não resolvidas por nenhum dos restantes mecanismos do Escudo de Proteção da Privacidade, se existentes.

A. **Âmbito de aplicação**

A presente opção de arbitragem encontra-se disponível para que os cidadãos determinem, no que se refere a queixas não resolvidas, se uma organização aderente ao Escudo de Proteção da Privacidade violou as suas obrigações nos termos dos princípios para com o cidadão em causa, e se tal violação continua total ou parcialmente por resolver. Esta opção encontra-se disponível apenas para estes efeitos. Esta opção não se encontra disponível, por exemplo, no que se refere às derrogações aos princípios ([1]) ou no respeitante a uma alegação sobre a adequação do Escudo de Proteção da Privacidade.

B. **Reparações disponíveis**

Ao abrigo desta opção de arbitragem, o Comité do Escudo de Proteção da Privacidade (constituído por um ou três árbitros, conforme o acordado pelas partes) têm competência para aplicar medidas equitativas, não monetárias e específicas do cidadão (tais como acesso, correção, eliminação ou devolução dos dados do cidadão em questão) necessárias para corrigir a violação dos princípios apenas no que se refere ao cidadão. Estes são os únicos poderes do comité de arbitragem no que diz respeito às reparações. Ao ponderar as reparações, o comité de arbitragem deve tomar em consideração outras reparações que já tinham sido aplicadas por outros mecanismos ao abrigo do Escudo de Proteção da Privacidade. Não se encontram disponíveis indemnizações, custos, taxas ou outras reparações. Cada parte suporta os honorários do próprio advogado.

C. **Requisitos prévios à arbitragem**

Um cidadão que decida invocar esta opção de arbitragem deve tomar as seguintes medidas antes de dar início a um pedido de arbitragem: 1) Expor a alegada violação diretamente à organização e conceder-lhe a oportunidade de resolver o problema no prazo estipulado na secção III, ponto 11, alínea d), subalínea i), dos princípios; 2) Utilizar o mecanismo de recurso independente ao abrigo dos princípios, que não acarreta custos para o indivíduo; e 3) Expor o problema através da sua autoridade responsável pela proteção dos dados ao *Department of Commerce* e permitir que este envide os seus melhores esforços para resolver o problema nos prazos estabelecidos na carta da *International Trade Administration* do *Department of Commerce*, sem custos para o cidadão.

A presente opção de arbitragem não pode ser invocada se a mesma alegada violação dos princípios apresentada pelo cidadão 1) tiver sido previamente objeto de arbitragem vinculativa; 2) tiver sido objeto de um acórdão final relativo a uma ação judicial da qual o cidadão fez parte; ou 3) tiver sido previamente objeto de um acordo entre as partes. Além disso, esta opção não pode ser invocada se uma autoridade responsável pela proteção dos dados da UE 1) tiver competência nos termos das secções III, ponto 5, ou III, ponto 9, dos princípios; ou 2) tiver competência para resolver a alegada violação diretamente junto da organização. A competência de uma APD para resolver a mesma queixa contra um responsável pelo tratamento de dados da UE não exclui, por si só, a invocação desta opção de arbitragem contra uma entidade jurídica diferente não vinculada pela autoridade da APD.

D. **Caráter vinculativo das decisões**

A decisão de um cidadão de invocar esta opção de arbitragem vinculativa é completamente voluntária. As decisões de arbitragem serão vinculativas para todas as partes na arbitragem. Depois de invocada, o cidadão abdica da opção de solicitar reparações pela mesma alegada violação noutro fórum, exceto que, se uma medida não monetária equitativa não resolver na íntegra a alegada violação, a invocação de arbitragem por parte do cidadão não exclui um pedido de indemnização disponível nos tribunais.

([1]) Secção I, ponto 5, dos princípios.

E. **Controlo e execução**

Os cidadãos e as organizações aderentes ao Escudo de Proteção da Privacidade poderão solicitar o controlo jurisdicional e a execução de decisões de arbitragem nos termos da legislação dos EUA ao abrigo da *Federal Arbitration Act* (lei relativa à arbitragem federal) ([1]). Todos os casos deste tipo devem ser apresentados no tribunal federal distrital cuja abrangência territorial inclua o principal estabelecimento da organização aderente ao Escudo de Proteção da Privacidade.

Esta opção de arbitragem destina-se a resolver litígios individuais e as decisões de arbitragem não visam funcionar como um precedente persuasivo ou vinculativo em questões que envolvam outras partes, designadamente em arbitragens futuras ou nos tribunais da UE ou dos EUA, nem em processos da FTC.

F. **O comité de arbitragem**

As partes selecionarão os árbitros a partir da lista de árbitros discutida abaixo.

Em conformidade com a legislação aplicável, o *Department of Commerce* dos EUA e a Comissão Europeia desenvolverão uma lista de pelo menos 20 árbitros, selecionados com base na independência, na integridade e em competências especializadas. É aplicável o seguinte em relação a este processo:

Árbitros:

1) permanecerão na lista durante um período de três anos, na ausência de circunstâncias excecionais ou justa causa, renovável durante um período adicional de três anos;

2) não devem receber quaisquer instruções de, nem estar associados a, qualquer parte, qualquer organização aderente ao Escudo de Proteção da Privacidade, aos EUA, à UE, a qualquer Estado-Membro da UE nem a qualquer outra autoridade governamental, autoridade pública ou organismo de execução; e

3) devem estar habilitados a exercer Direito nos EUA e ser peritos na legislação norte-americana relativa a privacidade, bem como ser especializados na legislação da UE em matéria de proteção de dados.

G. **Procedimentos de arbitragem**

Em conformidade com a legislação aplicável, no prazo de seis meses a contar da adoção da decisão de adequação, o *Department of Commerce* e a Comissão Europeia concordarão em adotar um conjunto existente e estabelecido de procedimentos de arbitragem norte-americanos (por exemplo, das entidades AAA ou JAMS) para regular os processos perante o Comité do Escudo de Proteção da Privacidade, sob reserva de cada uma das seguintes considerações:

1. Um cidadão pode dar início a arbitragem vinculativa, sob reserva da disposição acima relativa aos requisitos prévios à arbitragem, através da apresentação de um «aviso» à organização. O aviso deve conter um resumo das medidas tomadas nos termos do ponto C para resolver a queixa, uma descrição da alegada violação e, à escolha do cidadão, quaisquer documentos e materiais comprovativos e/ou uma discussão da legislação relativa à alegada queixa.

([1]) O capítulo 2 da *Federal Arbitration Act* («FAA») prevê que «[u]m acordo de arbitragem ou uma sentença arbitral decorrentes de uma relação jurídica, contratual ou não, que seja considerada comercial, nomeadamente uma transação, um contrato ou acordo descritos na [secção 2 do FAA], são abrangidos pela Convenção [sobre o Reconhecimento e a Execução de Sentenças Arbitrais Estrangeiras de 10 de junho de 1958, 21 U.S.T. 2519, T.I.A.S. N.º 6997 («Convenção de Nova Iorque»)]». 9 U.S.C. § 202. Além disso, o FAA estabelece que «[d]eve considerar-se que um acordo ou sentença decorrente de uma relação desse tipo exclusivamente entre cidadãos dos Estados Unidos não é abrangido pela Convenção [de Nova Iorque], a menos que a relação implique imóveis localizados no estrangeiro, preveja o cumprimento ou a execução no estrangeiro, ou tenha alguma relação razoável de outro tipo com um ou mais Estados estrangeiros». *Id.* Nos termos do capítulo 2, «qualquer parte na arbitragem pode solicitar a qualquer tribunal com competência no âmbito do presente capítulo um acórdão que confirme a sentença como contra qualquer outra parte na arbitragem. O tribunal deve confirmar a sentença, a menos que constate um dos motivos de recusa ou diferimento do reconhecimento ou da execução da sentença especificados na referida Convenção [de Nova Iorque]». *Id.* § 207. Além disso, o capítulo 2 estipula que «[O]s tribunais distritais dos Estados Unidos […] devem ter competência original sobre […] uma ação ou um processo [nos termos da Convenção de Nova Iorque], independentemente do montante em questão». *Id.* § 203.
O capítulo 2 estabelece ainda que o «capítulo 1 é aplicável às ações e aos processos instaurados nos termos do presente capítulo, desde que o referido capítulo não seja contrário ao presente capítulo ou à Convenção [de Nova Iorque], tal como ratificada pelos Estados Unidos». *Id.* § 208. O capítulo 1, por sua vez, estabelece que «[u]ma disposição por escrito num […] contrato que evidencie uma transação que implique trocas comerciais para resolver por arbitragem uma controvérsia decorrente de tal contrato ou transação, ou a recusa em executar o mesmo parcialmente ou na íntegra, ou um acordo por escrito para submeter a arbitragem uma controvérsia existente decorrente de um tal contrato, transação ou recusa, será válido, irrevogável e executório, salvo disposição em contrário na legislação ou nos tribunais para a revogação de qualquer contrato». *Id.* § 2. Além disso, o capítulo 1 estabelece que «qualquer parte na arbitragem pode solicitar ao tribunal assim especificado um acórdão que confirme a sentença e o tribunal deve emitir tal acórdão, a menos que a sentença seja abandonada, alterada ou corrigida, tal como prescrito nas secções 10 e 11 da [FAA]». *Id.* § 9.

2. Desenvolver-se-ão procedimentos para garantir que a mesma alegada violação de um cidadão não é alvo de reparações ou procedimentos duplicados.

3. A ação da FTC pode proceder em paralelo com a arbitragem.

4. Nenhuma autoridade representante dos EUA, da UE, de qualquer Estado-Membro da UE ou qualquer outra autoridade governamental, autoridade pública ou organismo de execução pode participar nestas arbitragens; contudo, mediante pedido de um cidadão da UE, as APD da UE podem prestar assistência na elaboração apenas do aviso, mas não podem ter acesso a conteúdos ou quaisquer outros materiais relacionados com estas arbitragens.

5. A arbitragem realizar-se-á nos Estados Unidos e o cidadão pode optar pela participação por videoconferência ou telefone, que será proporcionada sem custos para o cidadão. A participação em pessoa não será exigida.

6. A língua utilizada na arbitragem será o inglês, salvo acordo das partes em contrário. Mediante pedido fundamentado, e tomando em consideração se o cidadão é representado por um advogado, será fornecida interpretação na audição arbitral, bem como a tradução dos materiais de arbitragem, sem custos para o cidadão, a menos que o comité considere que, nas circunstâncias da arbitragem específica, tal conduziria a custos injustificados ou desproporcionados.

7. Os materiais apresentados aos árbitros serão tratados confidencialmente e serão utilizados apenas em relação à arbitragem.

8. Os conteúdos específicos do cidadão podem ser autorizados, se necessário, serão tratados confidencialmente pelas partes e serão utilizados apenas em relação à arbitragem.

9. A arbitragem deve ser concluída no prazo de 90 dias da apresentação do aviso à organização em questão, salvo acordo das partes em contrário.

H. **Custos**

Os árbitros devem tomar medidas razoáveis para minimizar os custos ou taxas das arbitragens.

Sob reserva da legislação aplicável, o *Department of Commerce* facilitará a instituição de um fundo, para o qual as organizações aderentes ao Escudo de Proteção da Privacidade serão obrigadas a pagar uma contribuição anual, baseada em parte na dimensão da organização, que abrangerá o custo de arbitragem, nomeadamente os honorários dos árbitros, até montantes máximos («limites»), em consulta com a Comissão Europeia. O fundo será gerido por um terceiro, que apresentará regularmente informações sobre o funcionamento do fundo. Na reapreciação anual, o *Department of Commerce* e a Comissão Europeia reapreciarão o funcionamento do fundo, designadamente a necessidade de ajustar o montante das contribuições ou dos limites e analisarão, entre outros elementos, o número de arbitragens, bem como os respetivos custos e calendarização, com o entendimento mútuo de que não será imposto um encargo financeiro excessivo sobre as organizações aderentes ao Escudo de Proteção da Privacidade. Os honorários dos advogados não são abrangidos pela presente disposição nem por qualquer fundo nos termos da presente disposição.

ANEXO II

PRINCÍPIOS DO QUADRO DO ESCUDO DE PROTEÇÃO DA PRIVACIDADE UE-EUA EMITIDOS PELO *DEPARTMENT OF COMMERCE* DOS EUA

I. VISÃO GERAL

1. Os Estados Unidos e a União Europeia, embora perfilhem o propósito comum de assegurar a proteção da vida privada, abordam a questão de formas diferentes. Os Estados Unidos recorrem a uma abordagem setorial com base numa mescla de legislação, regulamentação e autorregulamentação. Tomando em consideração estas diferenças e a fim de disponibilizar às organizações dos Estados Unidos um mecanismo fiável para as transferências de dados pessoais para os EUA a partir da União Europeia, assegurando ao mesmo tempo que os titulares de dados da UE continuam a beneficiar de proteção e garantias adequadas, tal como exigido pela legislação europeia no que se refere ao tratamento dos seus dados pessoais quando são transferidos para países não pertencentes à UE, o *Department of Commerce* emite os presentes princípios do Escudo de Proteção da Privacidade, designadamente os princípios suplementares (coletivamente «os princípios») ao abrigo da sua competência jurídica para fomentar, promover e desenvolver o comércio internacional (15 U.S.C. § 1512). Os princípios foram desenvolvidos com base em consultas com a Comissão Europeia e com o setor, bem como outras partes interessadas, para facilitar as relações comerciais e as transações entre os Estados Unidos e a União Europeia. Devem ser utilizados exclusivamente pelas organizações dos Estados Unidos que recebem dados pessoais da União Europeia para serem elegíveis para o Escudo de Proteção da Privacidade e, portanto, beneficiarem da decisão de adequação da Comissão Europeia ([1]). Os princípios não afetam a aplicação de disposições nacionais de aplicação da Diretiva 95/46/CE («a diretiva») em matéria de tratamento de dados pessoais nos Estados-Membros. Os princípios também não limitam as obrigações em matéria de proteção da privacidade de outro modo aplicáveis nos termos do direito dos EUA.

2. Para que se possam basear no Escudo de Proteção da Privacidade para efetuar transferências de dados pessoais da UE, as organizações devem autocertificar a sua adesão aos princípios ao *Department of Commerce* (ou ao seu representante). Portanto, embora a decisão das organizações de aderirem ao Escudo de Proteção da Privacidade seja estritamente voluntária, a conformidade efetiva é obrigatória: as organizações que autocertificam ao *Department of Commerce* e declaram publicamente o seu compromisso de aderir aos princípios devem cumpri-los na íntegra. Para aderir ao Escudo de Proteção da Privacidade, uma organização deve a) estar sujeita aos poderes de investigação e execução da *Federal Trade Commission* («FTC»), do *Department of Transportation* ou de outro organismo público que assegurará efetivamente a conformidade com os princípios *(no futuro, outros organismos públicos dos EUA reconhecidos pela UE podem figurar em anexo)*; b) declarar publicamente o seu compromisso de respeitar os princípios; c) divulgar publicamente as suas políticas em matéria de proteção da privacidade em conformidade com estes princípios; e d) aplicá-los na íntegra. O incumprimento por parte de uma organização é executório nos termos da Secção 5 da *Federal Trade Commission Act* que proíbe atos desleais e desonestos praticados no comércio [15 U.S.C. § 45, a)] ou de outra legislação ou regulamentação que proíba estes atos.

3. O *Department of Commerce* manterá e disponibilizará ao público uma lista oficial das organizações dos EUA que autocertificaram a sua adesão ao *Department of Commerce*, bem como o seu compromisso de aderir aos princípios («a lista do Escudo de Proteção da Privacidade»). Os benefícios do Escudo de Proteção da Privacidade são assegurados a partir da data em que o *Department of Commerce* inscreve a organização na lista de Proteção da Privacidade. O *Department of Commerce* suprimirá uma organização da lista do Escudo de Proteção da Privacidade se esta deixar de participar voluntariamente no referido quadro ou se não apresentar a sua recertificação anual ao *Department of Commerce*. A supressão de uma organização da lista do Escudo de Proteção da Privacidade significa que esta deixa de poder beneficiar da decisão de adequação da Comissão Europeia para receber informações pessoais da UE. A organização deve continuar a aplicar os princípios às informações pessoais que recebeu enquanto participava no Escudo de Proteção da Privacidade e confirmar anualmente ao *Department of Commerce* o seu compromisso de continuar a fazê-lo, enquanto preservar tais informações; caso contrário, a organização deve devolver ou eliminar as informações ou assegurar um nível de proteção «adequado» às informações através de outros meios autorizados. O *Department of Commerce* também suprimirá da lista do Escudo de Proteção da Privacidade as organizações que não tenham cumprido persistentemente os princípios; estas organizações não podem beneficiar do Escudo de Proteção da Privacidade e devem devolver ou eliminar as informações pessoais que receberam ao abrigo do Escudo de Proteção da Privacidade.

4. O *Department of Commerce* também manterá e disponibilizará ao público um registo oficial das organizações dos EUA que autocertificaram previamente a sua adesão ao *Department of Commerce*, mas que foram suprimidas da lista do Escudo de Proteção da Privacidade. O *Department of Commerce* apresentará um aviso claro de que estas organizações não participam no Escudo de Proteção da Privacidade; que a supressão da lista do Escudo de Proteção

([1]) Uma vez que a Decisão da Comissão sobre a adequação da proteção assegurada pelo Escudo de Proteção da Privacidade UE-EUA é aplicável à Islândia, ao Liechtenstein e à Noruega, o pacote do Escudo de Proteção da Privacidade abrangerá tanto a União Europeia como estes três países. Consequentemente, as remissões para a UE e os seus Estados-Membros devem ser entendidas como incluindo a Islândia, o Liechtenstein e a Noruega.

da Privacidade significa que estas organizações não podem alegar respeitar o Escudo de Proteção da Privacidade e devem evitar todas as declarações ou práticas enganosas que sugiram que participam no Escudo de Proteção da Privacidade; e que tais organizações já não têm direito a beneficiar da decisão de adequação da Comissão Europeia que lhes permitiria receber informações pessoais da UE. Uma organização que continue a alegar participar no Escudo de Proteção da Privacidade ou que apresente outras declarações falsas relacionadas com o Escudo de Proteção da Privacidade depois de ter sido suprimida da lista do referido quadro pode ser objeto de medidas de execução por parte da FTC, do *Department of Transportation* ou de outros organismos de execução.

5. A adesão a estes princípios 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, ou c) por exceção ou derrogação prevista na diretiva ou nas normas de direito interno dos Estados-Membros, desde que a aplicação das referidas exceções ou derrogações ocorra em contextos comparáveis. Para que se possa melhorar a proteção da vida privada, as organizações deverão envidar esforços no sentido de aplicar estes princípios de forma integral e transparente, incluindo a indicação das respetivas políticas de proteção da vida privada, sempre que as exceções aos princípios permitidas pela alínea b) *supra* se apliquem regularmente. Pela mesma razão, quando a escolha for permitida pelos princípios e/ou pela legislação norte-americana, as organizações deverão optar pelo nível de proteção mais elevado possível.

6. As organizações são obrigadas a aplicar os princípios a todos os dados pessoais transferidos com base no Escudo de Proteção da Privacidade após a adesão ao mesmo. Uma organização que opte por aplicar os princípios do Escudo de Proteção da Privacidade a informação pessoal relativa a recursos humanos transferida da UE, para utilização no contexto de relações laborais, deve indicá-lo na autocertificação apresentada ao *Department of Commerce*, em conformidade com o disposto no princípio suplementar sobre autocertificação.

7. Aplica-se o direito norte-americano às questões de interpretação e respeito dos princípios e outras medidas de proteção da vida privada praticadas pelas organizações aderentes ao Escudo de Proteção da Privacidade, à exceção de casos em que tais organizações se tenham comprometido a cooperar com as autoridades europeias responsáveis pela proteção dos dados («APD»). Salvo indicação em contrário, todas as disposições dos princípios são aplicáveis sempre que sejam relevantes.

8. Definições:

   a. «Dados pessoais» e «informação pessoal» são os dados que se referem a uma pessoa identificada ou identificável, que entrem no âmbito da diretiva e que, sendo provenientes da UE, sejam recebidos por entidades norte-americanas, independentemente da forma em que se encontrem registados.

   b. «Tratamento» de dados pessoais é qualquer operação ou conjunto de operações sobre dados pessoais, efetuadas com ou sem meios automatizados, tais como a recolha, o registo, a organização, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a comunicação ou difusão, e apagamento ou destruição.

   c. «Responsável pelo tratamento de dados», uma pessoa ou organização que, de forma autónoma ou em conjunto com outros, determina os objetivos e meios do tratamento de dados pessoais.

9. A data de entrada em vigor dos princípios é a data de aprovação final da determinação de adequação da Comissão Europeia.

II. PRINCÍPIOS

1. **Aviso**

   a. Uma organização deve informar os cidadãos quanto ao seguinte:

      i. a sua participação no Escudo de Proteção da Privacidade e fornecer uma ligação para a lista do Escudo de Proteção da Privacidade ou o respetivo sítio Web,

      ii. os tipos de dados pessoais recolhidos e, sempre que aplicável, as entidades ou filiais da organização que também aderem aos princípios,

iii. o seu compromisso de submeter aos princípios todos os dados pessoais recebidos da UE com base no Escudo de Proteção da Privacidade,

iv. os fins a que se destinam a recolha e utilização das informações pessoais que lhes dizem respeito,

v. a forma de contactar a organização para qualquer questão ou queixa, nomeadamente qualquer estabelecimento relevante na UE que possa responder a tais questões ou queixas,

vi. o tipo ou a identidade de terceiros a quem a informação pessoal é comunicada e os fins para os quais tal é realizado,

vii. o direito dos cidadãos de aceder aos seus dados pessoais,

viii. as opções e meios que a organização coloca à disposição dos cidadãos para limitarem a utilização e comunicação dos seus dados pessoais,

ix. o organismo independente para a resolução de litígios designado para resolver queixas e proporcionar vias de recurso gratuitas para o cidadão, e se é: 1) o painel instituído pelas APD, 2) um fornecedor de resolução alternativa de litígios sediado na UE, ou 3) uma entidade para a resolução alternativa de litígios sediada nos EUA,

x. ser objeto dos poderes de investigação e execução da FTC, do *Department of Transportation* ou de qualquer outro organismo público autorizado dos EUA,

xi. a possibilidade de, em determinadas condições, o cidadão solicitar arbitragem vinculativa,

xii. o requisito de comunicar informações pessoais em resposta a pedidos legais efetuados por autoridades públicas, designadamente para cumprir requisitos em matéria de segurança nacional ou aplicação da lei, e

xiii. a sua responsabilidade em caso de transferências ulteriores para terceiros.

b. Este aviso deve ser formulado em linguagem clara e de forma bem visível 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.

2. **Escolha**

a. Uma organização deve facultar aos cidadãos a possibilidade de escolher («*opt out*» — opção de não participação) se os seus dados pessoais podem: i) ser divulgados a terceiros, ou ii) ser utilizados para fins significativamente diferentes dos que presidiram à recolha inicial ou dos que foram subsequentemente autorizados pelas pessoas em causa. Para poderem optar, as pessoas devem ter acesso a mecanismos claros, transparentes e facilmente disponíveis.

b. Em derrogação do número anterior, não é necessário aplicar o princípio de escolha quando a informação é divulgada a um agente subcontratado para desempenhar tarefas em nome e segundo instruções da organização. Porém, as organizações devem celebrar sempre um contrato com o agente.

c. Para a recolha de informações de natureza mais sensível (informações pessoais relativas a condições de saúde ou doenças, origem racial ou étnica, opiniões políticas, crenças religiosas ou filosóficas, pertença a sindicatos ou informações relativas à vida sexual da pessoa), as organizações devem obter a autorização afirmativa expressa no sentido da participação («*opt in*») dos cidadãos, caso se pretenda i) divulgar a informação a terceiros ou ii) utilizá-la para um fim diferente do que, inicialmente, motivou a sua recolha ou do fim subsequentemente autorizado pelas pessoas através do exercício da opção de participação. Além disso, qualquer informação pessoal recebida de terceiros, que estes tratem e considerem como sendo de natureza sensível, deverá ser tratada como tal pela organização destinatária.

3. **Responsabilização pela transferência ulterior**

a. Para poderem transferir informações pessoais para terceiros na qualidade de responsáveis pelo tratamento de dados, as organizações deverão aplicar os princípios de aviso e escolha. As organizações também devem celebrar um contrato com um terceiro responsável pelo tratamento de dados que preveja que tais dados podem ser tratados apenas para fins limitados e especificados em consonância com o consentimento dado pela pessoa em causa e que o destinatário assegurará o mesmo nível de proteção que os princípios e notificará a organização se se determinar que já não pode cumprir esta obrigação. O contrato deve prever que, quando efetuada essa determinação, o terceiro responsável pelo tratamento dos dados cessa o tratamento ou tome outras medidas razoáveis para remediar a situação.

b. Para poderem transferir dados pessoais para um terceiro que desempenhe a função de agente, as organizações devem fazer o seguinte: i) transferir os dados referidos para fins limitados e específicos; ii) garantir que o agente é obrigado a assegurar, pelo menos, o mesmo nível de proteção da privacidade que o exigido pelos princípios; iii) tomar medidas razoáveis e adequadas para garantir que o agente trata de modo eficaz as informações pessoais transferidas de forma coerente com as obrigações da organização nos termos dos princípios; iv) impor ao agente que notifique a organização se se determinar que já não pode cumprir a obrigação de assegurar o mesmo nível de proteção previsto nos princípios; v) após aviso, também no quadro da alínea iv), tomar medidas razoáveis e adequadas para cessar e corrigir o tratamento não autorizado; e, vi) apresentar ao *Department of Commerce*, mediante pedido, um resumo ou uma cópia representativa das disposições relevantes em matéria de proteção da privacidade do seu contrato com esse agente.

4. **Segurança**

a. As organizações que criam, conservam, utilizam ou divulgam informações pessoais devem tomar medidas razoáveis e adequadas para evitar a perda, utilização indevida e acesso, revelação, alteração ou destruição não autorizados, tomando em devida consideração os riscos inerentes ao tratamento e à natureza dos dados pessoais.

5. **Integridade dos dados e limitação dos objetivos**

a. De acordo com os princípios, as informações pessoais devem ser limitadas às informações que são relevantes para os objetivos do tratamento ([1]). Uma organização não pode tratar informações pessoais de um modo incompatível com os objetivos que motivaram a recolha ou com os objetivos autorizados posteriormente pelo pessoa em causa. Na medida necessária para se atingirem esses objetivos, as organizações devem tomar providências razoáveis para garantir a fiabilidade dos dados pessoais em função da utilização prevista, bem como se são exatos, completos e atuais. As organizações devem respeitar os princípios enquanto conservarem tais informações.

b. As informações podem ser conservados sob uma forma identificável ([2]) ou de identificação individual enquanto serve uma finalidade de tratamento na aceção do n.º 5-A. Esta obrigação não obsta a que as organizações trate dados pessoais por períodos mais longos, durante o tempo e na medida em que esse tratamento seja razoavelmente funcional a objetivos como o arquivo no interesse público, a atividade jornalística, literária e artística, a investigação científica ou histórica e a análise estatística. Nestes casos, o tratamento deve estar sujeito a outros princípios e disposições do quadro. As organizações devem tomar medidas razoáveis e adequadas para dar cumprimento a esta disposição.

6. **Acesso**

a. Os cidadãos devem poder ter acesso às informações pessoais que lhes dizem respeito e que estejam na posse de uma organização; devem poder retificar, alterar ou eliminar informações inexatas, ou que tenham sido tratadas em violação dos princípios, salvo se os encargos ou as despesas para facultar esse acesso forem desproporcionados em relação aos riscos para a vida privada da pessoa em causa, ou sempre que os legítimos direitos de terceiros incorram em risco de violação.

([1]) Consoante as circunstâncias, podem constituir exemplos de objetivos de tratamento compatíveis os que são razoavelmente funcionais às relações com os clientes, as considerações jurídicas e de conformidade, as atividades de auditoria, a segurança e a prevenção da fraude, a preservação e defesa dos direitos jurídicos da organização ou outros objetivos coerentes com as expectativas de uma pessoa razoável, tendo em conta o contexto em que se inscreve a recolha.

([2]) Neste contexto, a pessoa é «identificável» se, tendo em conta os meios de identificação suscetíveis de serem razoavelmente utilizados (atendendo, nomeadamente, aos custos e ao tempo necessário para a identificação e à tecnologia disponível no momento do tratamento) e o formato em que os dados são conservados, a organização ou um terceiro que tenha acesso aos dados poderiam razoavelmente identificar a pessoa.

7. **Recurso, aplicação e responsabilidade**

a. A proteção efetiva da vida privada deve incluir mecanismos sólidos que garantam o cumprimento dos princípios, recursos para os cidadãos que tenham sido afetados pelo incumprimento dos princípios, bem como consequências para as organizações sempre que os princípios não sejam seguidos. Estes mecanismos devem incluir, no mínimo:

i. mecanismos de recurso independentes e imediatamente disponíveis através dos quais as queixas e os litígios dos cidadãos possam ser investigados e resolvidos de forma célere sem custos para os cidadãos e com referência aos princípios, e os danos reparados sempre que a lei aplicável ou as iniciativas do setor privado o prevejam;

ii. procedimentos de acompanhamento para indagar da veracidade das atestações e alegações das organizações em relação às suas práticas em matéria de proteção da vida privada e para verificar se essas práticas relativas à vida privada foram executadas da forma apresentada e, em especial, no que se refere aos casos de incumprimento; e

iii. a obrigação de solucionar problemas decorrentes do incumprimento dos princípios por organizações que tenham anunciado a sua adesão e consequências para essas organizações. As sanções devem ser suficientemente rigorosas de modo a garantirem o cumprimento por parte das organizações.

b. As organizações e os respetivos mecanismos de recurso independentes selecionados responderão imediatamente às questões e aos pedidos de informações apresentados pelo *Department of Commerce* sobre o Escudo de Proteção da Privacidade. Todas as organizações devem responder com celeridade às queixas relativas à conformidade com os princípios transmitidas pelas autoridades dos Estados-Membros da UE através do *Department of Commerce*. As organizações que tenham optado por colaborar com as APD, nomeadamente as organizações que procedem ao tratamento de dados relativos a recursos humanos, devem responder diretamente a tais autoridades no que diz respeito à investigação e resolução de queixas.

c. As organizações são obrigadas a proceder à arbitragem de queixas e a seguir as condições estabelecidas no anexo I, desde que um cidadão tenha solicitado arbitragem vinculativa mediante a apresentação de um aviso à organização em questão, de acordo com os procedimentos estipulados no anexo I e sob reserva das condições aí estabelecidas.

d. No contexto de uma transferência ulterior, as organizações aderentes ao Escudo de Proteção da Privacidade são responsáveis pelo tratamento das informações pessoais que recebem ao abrigo do Escudo de Proteção da Privacidade e transferem posteriormente para um terceiro que desempenha a função de agente em seu nome. A organização aderente ao Escudo de Proteção da Privacidade deve permanecer responsável nos termos dos princípios se o seu agente proceder ao tratamento de tais informações pessoais de forma incompatível com os princípios, a menos que a organização prove que não é responsável pela situação conducente aos danos.

e. Sempre que uma organização seja objeto de uma decisão judicial ou da FTC por motivo de incumprimento, a organização deve publicar todas as secções relevantes relacionadas com o Escudo de Proteção da Privacidade dos relatórios de conformidade ou avaliação apresentados à FTC, de acordo com os requisitos de confidencialidade. O *Department of Commerce* criou um ponto de contacto dedicado ao qual as APD podem recorrer em caso de problemas de conformidade por parte das organizações aderentes ao Escudo de Proteção da Privacidade. A FTC dará prioridade às queixas de incumprimento dos princípios recebidas do *Department of Commerce* e das autoridades dos Estados-Membros da UE e procederá ao intercâmbio de informações sobre estas queixas com as autoridades públicas em questão em tempo útil, sob reserva das restrições existentes em termos de confidencialidade.

III. PRINCÍPIOS SUPLEMENTARES

1. **Dados sensíveis**

a. As organizações não são obrigadas a obter uma autorização afirmativa expressa (opção de participação) no que diz respeito aos dados sensíveis se o tratamento dos dados:

i. se realizar em função de interesses vitais da pessoa em causa ou de outra pessoa;

ii. for necessário para a preparação de recursos ou processos judiciais;

iii. for necessário para prestar cuidados médicos ou elaborar um diagnóstico;

iv. for efetuado no decurso das atividades legítimas de uma fundação, associação ou qualquer outro organismo sem fins lucrativos que possua objetivos políticos, filosóficos, religiosos ou sindicais, na condição de que o tratamento se refira exclusivamente aos membros do organismo ou às pessoas que com ele mantenham contactos habituais no âmbito dos referidos objetivos, e de que os dados não sejam revelados a terceiros sem o consentimento dos titulares de dados;

v. for necessário para que a entidade cumpra as suas obrigações em matéria de direito do trabalho, ou

vi. se referir a informação publicada pela pessoa em causa.

2. **Exceções jornalísticas**

a. Tendo em conta a liberdade de imprensa garantida pela Constituição dos EUA, bem como as isenções em matéria de jornalismo previstas pela diretiva, sempre que o direito de liberdade de imprensa consagrado na Primeira Emenda da Constituição dos EUA não for compatível com os interesses de proteção da vida privada, a Primeira Emenda deverá garantir o equilíbrio de tais interesses no que diz respeito às atividades de pessoas ou de organizações norte-americanas.

b. A informação pessoal recolhida para efeitos de publicação, difusão ou outra forma de comunicação pública de material jornalístico, quer seja, ou não, utilizada, bem como a informação constante de material já publicado e arquivado, não está sujeita aos requisitos dos princípios do Escudo de Proteção da Privacidade.

3. **Responsabilidade subsidiária**

a. Os fornecedores de serviços da Internet (ISP), os operadores de telecomunicações e outras organizações não estão sujeitos aos princípios do Escudo de Proteção da Privacidade quando, em nome de outra organização, se limitam a transmitir, encaminhar, trocar ou guardar informação. À semelhança da própria diretiva, o Escudo de Proteção da Privacidade não gera uma responsabilidade subsidiária. Não se poderá responsabilizar uma entidade que aja exclusivamente como transmissora de dados transmitidos por terceiros e não seja determinante nem para a finalidade, nem para os meios de tratamento dos dados pessoais.

4. **Realizar auditorias e auditorias jurídicas**

a. As atividades de auditores e bancos de investimento podem implicar o tratamento de dados pessoais sem conhecimento do interessado. Os princípios de aviso, escolha e acesso permitem este tipo de tratamento nos casos descritos abaixo.

b. As sociedades de capitais públicos e as sociedades com caráter fechado, nomeadamente as organizações aderentes ao Escudo de Proteção da Privacidade, são regularmente objeto de auditorias. Estas auditorias, designadamente as que investigam potenciais irregularidades, podem ser prejudicadas se forem divulgadas prematuramente. Igualmente, uma organização do Escudo de Proteção da Privacidade envolvida numa potencial fusão ou aquisição necessitará de proceder a uma auditoria jurídica ou ser objeto da mesma. Isto implicará muitas vezes a recolha e o tratamento de dados pessoais, tais como informações sobre os quadros superiores e outro pessoal importante. A divulgação prematura poderia impedir a transação ou poderia mesmo violar a regulamentação aplicável às sociedades de valores. Os bancos de investimento e os advogados envolvidos em auditorias jurídicas, ou os auditores que realizam auditorias, podem tratar informação sem conhecimento do interessado, apenas na medida em que isso se justifique, e pelo tempo necessário, em função de disposições regulamentares ou por razões de interesse público, bem como noutras circunstâncias em que a aplicação desses princípios seja prejudicial aos interesses legítimos das suas organizações. Esses interesses incluem a verificação do cumprimento, por parte das organizações, das suas obrigações legais e atividades contabilísticas legítimas, e a observação da confidencialidade no contexto de possíveis aquisições, fusões, empresas comuns ou transações semelhantes efetuadas por bancos de investimento ou auditores.

5. **O papel das autoridades responsáveis pela proteção dos dados**

a. As organizações aplicarão o seu compromisso de cooperação com as autoridades europeias responsáveis pela proteção dos dados (APD) do modo descrito abaixo. Em conformidade com o Escudo de Proteção da Privacidade, as organizações norte-americanas que recebam dados pessoais provenientes da UE devem comprometer-se a utilizar mecanismos eficazes que garantam o cumprimento dos referidos princípios. Mais especificamente, tal como estabelecido no princípio de recurso, aplicação e responsabilidade, as organizações participantes devem proporcionar o seguinte: a), i), vias de recurso para as pessoas em causa; a, ii) procedimentos de acompanhamento, a fim de verificar a veracidade das afirmações e declarações das organizações em matéria de respeito da vida privada; e a), iii) a obrigação de as referidas organizações solucionarem os problemas que surjam por incumprimento dos princípios, bem como de assumirem as respetivas consequências. Uma organização pode satisfazer a alínea a), subalíneas i) e iii), previstas pelo princípio de recurso, aplicação e responsabilidade, comprometendo-se a cooperar com as APD, nas condições aqui estabelecidas.

b. Uma organização compromete-se a cooperar com as APD declarando na sua autocertificação de adesão ao Escudo de Proteção da Privacidade dirigida ao *Department of Commerce* (*ver* princípio suplementar sobre autocertificação) que:

i. opta por cumprir a alínea a), subalíneas i) e iii) do princípio de recurso, aplicação e responsabilidade do Escudo de Proteção da Privacidade, comprometendo-se a cooperar com as APD;

ii. cooperará com as APD na investigação e resolução de queixas formuladas no âmbito do Escudo de Proteção da Privacidade; e

iii. respeitará as decisões das APD, sempre que estas considerem que a organização deve tomar medidas específicas para cumprir os princípios do Escudo de Proteção da Privacidade, incluindo o pagamento de indemnizações ou compensações às pessoas prejudicadas pelo desrespeito dos princípios, e apresentará às APD confirmação por escrito de que tais medidas foram tomadas.

c. Funcionamento dos painéis das APD

i. A cooperação com as APD assumirá as formas de informação e aconselhamento seguintes:

1. O aconselhamento das APD será veiculado através de um painel das APD informal composto por estas autoridades à escala europeia, que contribuirá, entre outros aspetos, para assegurar uma abordagem coerente e harmonizada destas questões.

2. O painel deverá prestar aconselhamento às organizações norte-americanas no que respeita a queixas por resolver apresentadas pelas pessoas cuja informação pessoal, transferida da UE ao abrigo do Escudo de Proteção da Privacidade tenha sido objeto de tratamento. Esse aconselhamento, que tem por fim garantir a correta aplicação dos princípios do Escudo de Proteção da Privacidade, contemplará todas as vias de recurso para a(s) pessoa(s) em causa que as APD considerem adequadas.

3. O painel prestará aconselhamento em resposta a queixas trazidas pelas organizações em questão e/ou a queixas apresentadas diretamente por particulares contra as organizações que se tenham comprometido a cooperar, para efeitos do cumprimento do Escudo de Proteção da Privacidade, com as APD; estas incentivarão e, se necessário, auxiliarão as pessoas em causa a recorrer, em primeira instância, aos mecanismos internos de resolução de queixas de que as organizações disponham.

4. A resposta será emitida após ter sido dada a ambas as partes envolvidas a oportunidade de fornecer todas as informações e provas que considerem necessárias. O painel procurará responder o mais rapidamente possível, dentro dos limites processuais permitidos. Regra geral, o painel procurará responder nos 60 dias seguintes à receção da queixa e, se possível, antes de findo esse prazo.

5. Caso considere adequado, o painel publicará os resultados da análise das queixas recebidas.

6. O aconselhamento facultado em nada responsabiliza o painel no seu conjunto ou as APD individuais que o compõem.

ii. Como referido acima, as organizações que optem por esta solução para a resolução de litígios deverão ainda comprometer-se a respeitar as decisões das APD. Se as organizações não aplicarem o conselho da APD num prazo de 25 dias, sem apresentar uma razão válida para o atraso, o painel comunicará a sua intenção de submeter o assunto à apreciação da *Federal Trade Commission*, do *Department of Transportation* ou de outro organismo federal ou estadual norte-americano com competência para tomar medidas de execução em caso de fraude ou prestação de falsas declarações, ou para concluir que o acordo de cooperação foi seriamente quebrado devendo, por isso, ser considerado nulo. Nesta última hipótese, o painel informará o *Department of Commerce* e para que altere a lista do Escudo de Proteção da Privacidade em conformidade. Qualquer violação do acordo de cooperação com as APD, bem como dos princípios do Escudo de Proteção da Privacidade, será objeto de recurso ao abrigo da secção 5 da *FTC Act* (lei relativa à Comissão reguladora do comércio federal) (ou de outra lei semelhante.

d. Se a organização desejar que a sua adesão ao Escudo de Proteção da Privacidade abranja também os dados relativos a recursos humanos transferidos da UE para serem utilizados num contexto de relações laborais deve comprometer-se a colaborar com as APD no que diz respeito a esses dados (*ver* princípio suplementar sobre dados relativos a recursos humanos).

e. As organizações que escolherem esta opção deverão pagar uma taxa anual destinada aos custos de funcionamento do painel, podendo ainda ter que pagar quaisquer despesas de tradução necessárias, decorrentes das decisões do painel sobre as queixas de que são objeto. A taxa anual não excederá 500 dólares dos Estados Unidos (USD), sendo inferior para empresas de menor dimensão.

6. **Autocertificação**

a. Os benefícios decorrentes da adesão ao Escudo de Proteção da Privacidade vigoram a partir da data em que o *Department of Commerce* inclui a declaração de autocertificação da organização na lista do Escudo de Proteção da Privacidade após determinar que esta se encontra completa.

b. Para proceder à autocertificação de adesão ao Escudo de Proteção da Privacidade, as organizações devem apresentar ao *Department of Commerce* uma declaração de autocertificação assinada por um dos responsáveis da organização aderente ao Escudo de Proteção da Privacidade, em nome desta, contendo, no mínimo, a seguinte informação:

i. Designação da organização, endereço postal e de correio eletrónico, números de telefone e fax;

ii. Descrição das atividades da organização em matéria de informação pessoal recebida da UE; e

iii. Descrição da política em matéria de proteção da vida privada da organização no que diz respeito a essa informação pessoal, nomeadamente:

1. se a organização dispuser de um sítio Web público, o endereço Web relevante onde a política em matéria de proteção da privacidade se encontra disponível, ou se a organização não dispuser de um sítio Web público, o local onde o público pode consultar a política em matéria de proteção da privacidade;

2. a sua data de aplicação;

3. o nome do gabinete de contacto para a resolução de queixas, pedidos de acesso ou quaisquer outros assuntos relacionados com o Escudo de Proteção da Privacidade;

4. os organismos oficiais concretos com competência para deliberar sobre quaisquer queixas contra a organização em matéria de possíveis práticas desleais ou desonestas e violações das leis ou normas que regulamentam a proteção da vida privada (e que se encontram referidos nos princípios ou num futuro anexo dos princípios);

5. a designação de qualquer programa relativo à proteção da vida privada em que a organização participe;

6. o método de verificação (*por exemplo*, interno ou por terceiros) (*ver* princípio suplementar em matéria de verificação); e

7. o mecanismo de recurso independente que possa ser utilizado para investigar as queixas por resolver.

c. Se a organização desejar que a sua adesão ao Escudo de Proteção da Privacidade abranja também a informação relativa a recursos humanos transferida da UE para ser utilizada num contexto de relações laborais pode fazê-lo, desde que um organismo oficial referido nos princípios ou num anexo dos princípios tenha competência para conhecer de queixas contra a referida organização, decorrentes do tratamento de informações relativas a recursos humanos. Além disso, deve declarar na sua declaração de autocertificação que deseja abranger esse tipo de informações, que deseja colaborar com as autoridades da UE, em conformidade com os princípios suplementares relativos a dados sobre recursos humanos e o papel das autoridades responsáveis pela proteção dos dados, consoante o caso, e que acatará o parecer emitido por essas autoridades. A organização deve ainda fornecer ao *Department of Commerce* uma cópia da sua política em matéria de proteção da privacidade dos recursos humanos e apresentar informações sobre onde os trabalhadores em causa podem consultá-la.

d. O *Department of Commerce* manterá uma lista de todas as organizações aderentes ao Escudo de Proteção da Privacidade que apresentem declarações de autocertificação completas, garantindo desta forma a disponibilidade dos benefícios daí decorrentes, que atualizará com base nas notificações e declarações de renovação da certificação anuais recebidas, de acordo com o princípio suplementar sobre resolução de litígios e aplicação. Estas declarações de autocertificação deverão ser apresentadas, no mínimo, uma vez por ano; caso contrário, as organizações serão suprimidas da lista e deixarão de usufruir dos benefícios decorrentes do Escudo de Proteção da Privacidade. Tanto a lista do Escudo de Proteção da Privacidade como as declarações de autocertificação apresentadas pelas organizações serão colocadas à disposição do público. Todas as organizações que são inscritas na lista do Escudo de Proteção da Privacidade deverão também mencionar nas respetivas declarações públicas relativas à sua política em matéria de proteção da vida privada que aderem aos princípios do referido quadro.

Caso se encontre disponível em linha, a política em matéria de proteção da vida privada de uma organização deve incluir uma hiperligação para o sítio Web do *Department of Commerce*relativo ao Escudo de Proteção da Privacidade e uma hiperligação para o sítio Web ou um formulário de apresentação de queixas do mecanismo de recurso independente que pode ser utilizado para investigar queixas por resolver.

e. Os princípios de privacidade são aplicáveis imediatamente após a certificação. Reconhecendo que os princípios afetarão as relações comerciais com terceiros, as organizações que certificam a sua adesão ao quadro do Escudo de Proteção da Privacidade, nos primeiros dois meses a contar da data de entrada em vigor do quadro, devem adaptar as relações comerciais existentes com terceiros para cumprir o princípio de responsabilidade pela transferência ulterior logo que possível e, em todo o caso, o mais tardar nove meses a contar da data em que certificam a sua adesão ao Escudo de Proteção da Privacidade. Durante esse período transitório, sempre que as organizações transfiram dados para terceiros, devem i) aplicar os princípios de aviso e escolha e ii) sempre que sejam transferidos dados pessoais para um terceiro que desempenhe funções de agente, determinar que o agente é obrigado a assegurar pelo menos o mesmo nível de proteção que o exigido pelos princípios.

f. A organização deve submeter aos princípios do Escudo de Proteção da Privacidade todos os dados pessoais recebidos da UE ao abrigo do mesmo. O compromisso de adesão aos princípios do Escudo de Proteção da Privacidade não se limita apenas aos dados pessoais recebidos durante o período em que a organização usufrui dos benefícios daí decorrentes, já que, ao aderir, a organização se compromete a aplicar os ditos princípios aos dados em questão enquanto os armazenar, utilizar ou revelar, mesmo que, posteriormente, decida por qualquer motivo abandonar o Escudo de Proteção da Privacidade. Uma organização que abandone o Escudo de Proteção da Privacidade, mas que deseje preservar os referidos dados, deve confirmar anualmente ao *Department of Commerce* o seu compromisso de continuar a aplicar os princípios ou proporcionar uma proteção «adequada» das informações através de outros meios autorizados (por exemplo, através de um contrato que reflita na íntegra os requisitos das cláusulas contratuais-tipo relevantes adotadas pela Comissão Europeia); caso contrário, a organização deve devolver ou eliminar as informações. Uma organização que abandone o Escudo de Proteção da Privacidade deve suprimir da política relevante em matéria de proteção da vida privada todas as referências ao referido quadro que sugiram que a organização continua a participar ativamente no Escudo de Proteção da Privacidade e tem direito aos seus benefícios.

g. Uma organização que cesse como entidade jurídica separada, na sequência de uma fusão ou de uma aquisição, deve antecipadamente informar desse facto o *Department of Commerce*. A notificação deve ainda indicar se a nova entidade resultante da fusão ou da aquisição: i) continuará abrangida pelos princípios Escudo de Proteção da Privacidade por força do instrumento legal que regulou a fusão ou aquisição, ou ii) decide autocertificar a sua adesão aos princípios do Escudo de Proteção da Privacidade ou aplicar outro tipo de garantias, como um acordo escrito que garanta a adesão aos princípios. Quando nenhuma destas duas condições, i) e ii), se aplicar, quaisquer dados pessoais que tenham sido recebidos no âmbito do Escudo de Proteção da Privacidade devem ser prontamente eliminados.

h. Sempre que uma organização abandone o Escudo de Proteção da Privacidade por algum motivo, deve suprimir todas as declarações que sugiram que a organização continua a participar no referido quadro ou que tem direito aos benefícios daí decorrentes. A marca de certificação do Escudo de Proteção da Privacidade UE-EUA, se utilizada, também deve ser removida. Qualquer declaração falsa prestada ao público relativa à adesão de uma organização aos princípios do Escudo de Proteção da Privacidade poderá ser objeto de recurso junto da FTC ou de qualquer outra instância governamental competente. As declarações falsas prestadas ao *Department of Commerce* poderão ser objeto de recurso ao abrigo da *False Statements Act* (legislação sobre falsos testemunhos — 18 USC § 1001).

7. **Verificação**

a. As organizações devem prever modalidades de acompanhamento para verificar não só se os certificados e as declarações das empresas sobre as suas práticas em matéria de privacidade, no âmbito do Escudo de Proteção da Privacidade, correspondem à verdade, como também se essas práticas em matéria de privacidade foram aplicadas em conformidade com as declarações prestadas e com os princípios do Escudo de Proteção da Privacidade.

b. Para cumprir os requisitos de verificação do princípio de recurso, aplicação e responsabilidade, uma organização deve verificar os certificados e as declarações recorrendo quer a uma autoavaliação quer a verificações de conformidade externas.

c. No caso da autoavaliação, esta verificação deve indicar se a política pública da organização em matéria de proteção da vida privada no que respeita à informação pessoal recebida da UE é exata, abrangente, claramente exposta, completamente aplicada e acessível. Além disso, deverá indicar que a sua política em matéria de proteção da vida privada está conforme aos princípios do Escudo de Proteção da Privacidade; que as pessoas estão informadas sobre os instrumentos internos específicos de que a organização dispõe para processar as queixas e sobre os mecanismos independentes de apresentação de queixas; que a organização instituiu procedimentos específicos, que os trabalhadores receberam formação adequada para a sua aplicação e que se aplicam sanções em caso de não cumprimento dos mesmos; e, por fim, que estão em vigor procedimentos internos para

a realização periódica de verificações objetivas de conformidade com o acima exposto. A declaração de verificação da autoavaliação, que deverá ser assinada por um responsável da empresa, ou por qualquer outro representante autorizado, deve ser efetuada, no mínimo, uma vez por ano e posta à disposição das pessoas, mediante pedido ou no âmbito de uma investigação ou de queixa por motivos de não conformidade.

d. Se a organização tiver optado por verificações de conformidade externas, essas verificações deverão atestar que a sua política em matéria de proteção da vida privada no que respeita à informação pessoal recebida da UE é conforme aos princípios do Escudo de Proteção da Privacidade e está a ser devidamente cumprida, e que as pessoas são informadas dos mecanismos ao seu dispor para apresentar queixa. Os métodos de verificação poderão compreender, consoante os casos, sem restrições, auditorias, verificações aleatórias, o recurso a simulações ou o uso de instrumentos tecnológicos. A declaração atestando a realização da verificação de conformidade externa, que deverá ser assinada pelo responsável da verificação ou pelo responsável da empresa ou um outro representante autorizado, deve ser efetuada, no mínimo, uma vez por ano, e posta à disposição das pessoas, mediante pedido ou no âmbito de uma investigação ou queixa relativa à conformidade.

e. As organizações devem manter registos relativos à aplicação das suas práticas em matéria de privacidade no âmbito do Escudo de Proteção da Privacidade, que devem ser postos à disposição, mediante pedido, no âmbito de uma investigação ou queixa relativa à conformidade, da entidade independente responsável pela investigação da queixa ou da agência responsável em matéria de práticas desleais e desonestas. As organizações devem ainda responder imediatamente a questões ou outros pedidos de informações do *Department of Commerce* sobre a adesão da organização aos princípios.

8. **Acesso**

a. O princípio de acesso na prática

i. No âmbito dos princípios do Escudo de Proteção da Privacidade, o direito de acesso é fundamental para a proteção da vida privada. Permite, em especial, que as pessoas verifiquem a exatidão das informações que outras entidades possuem a seu respeito. O princípio de acesso significa que os cidadãos tem direito a:

1. obter de uma organização a confirmação de se a organização procede ao tratamento dos seus dados pessoais ([1]);

2. que lhes sejam comunicados esses dados a fim de poderem verificar a sua exatidão e a legalidade do tratamento; e

3. que os dados sejam corrigidos, alterados ou eliminados sempre que estejam incorretos ou sejam tratados em infração aos princípios.

ii. As pessoas não são obrigadas a justificar um pedido de acesso aos seus dados pessoais. Ao satisfazer os pedidos de acesso por parte das pessoas, as organizações devem guiar-se, em primeiro lugar, pelas preocupações que deram lugar ao pedido. Por exemplo, se um pedido de acesso é vago ou muito geral, a organização poderá entrar em diálogo com o interessado, a fim de tentar compreender qual a motivação subjacente ao pedido e poder prestar as informações adequadas. A organização pode desejar saber qual, ou quais, dos seus serviços a pessoa contactou ou a natureza da informação ou a sua utilização que é objeto do pedido de acesso.

iii. Uma vez que o princípio de acesso é fundamental, as organizações devem sempre, de boa-fé, envidar todos os esforços para conceder o acesso. Nos casos em que determinada informação exija proteção e se distinga com facilidade de outra informação pessoal que seja objeto de um pedido de acesso, a organização deverá reter a informação protegida e disponibilizar os restantes dados. Se uma organização decidir restringir o acesso em qualquer circunstância, deverá prestar à pessoa que o solicitou a devida justificação e informação sobre os contactos a efetuar para posteriores investigações.

b. Encargos ou despesas para facultar o acesso

i. O direito de acesso aos dados pessoais pode ser limitado em circunstâncias excecionais sempre que os legítimos direitos de terceiros incorram em risco de violação ou os encargos ou as despesas para facultar esse acesso forem desproporcionados em relação aos riscos para a vida privada da pessoa em causa. As despesas e os encargos são fatores importantes a ter em conta, embora não sejam fatores determinantes para avaliar a razoabilidade de um pedido de acesso.

([1]) A organização deve responder a questões dos cidadãos relativamente aos fins do tratamento, às categorias de dados pessoais em causa e aos destinatários ou categorias de destinatários aos quais os dados pessoais são divulgados.

ii. Se a informação pessoal é utilizada para tomar decisões que poderão afetar significativamente a pessoa em questão (por exemplo, a recusa ou concessão de benefícios consideráveis como seguros, hipotecas ou um emprego), a organização terá, em conformidade com as restantes disposições destes princípios suplementares, de divulgar a referida informação, mesmo que isso se revele relativamente difícil ou dispendioso. Se as informações pessoais solicitadas não forem de caráter sensível, nem forem utilizadas para tomar decisões que afetem consideravelmente a pessoa, mas a sua disponibilização for fácil e pouco dispendiosa, a organização deve facultar o acesso a essas informações.

c. Informações comerciais confidenciais

i. As informações comerciais confidenciais são dados relativamente aos quais uma organização toma medidas de proteção para que não sejam divulgados, sempre que possam ser utilizados para beneficiar a concorrência. As organizações podem recusar ou limitar o acesso na medida em que o pleno acesso implique revelar informações comerciais confidenciais a seu respeito, como é o caso das deduções ou classificações de *marketing* produzidas pela organização, ou informações comerciais confidenciais de terceiros que sejam objeto de uma obrigação contratual de confidencialidade.

ii. Nos casos em que a informação comercial confidencial se distinga com facilidade de outra informação pessoal que seja objeto de um pedido de acesso, a organização deverá reter a informação comercial confidencial e disponibilizar a que não é confidencial.

d. Organização de bases de dados

i. O acesso pode ser garantido sob a forma de prestação de informações pessoais relevantes por uma organização ao requerente, sem que haja necessidade de lhe conceder o acesso à base de dados da organização.

ii. O acesso apenas tem de ser concedido na medida em que a organização armazene a informação pessoal. O princípio de acesso não deve, por si, criar qualquer obrigação de recolha, manutenção, reorganização ou reestruturação de ficheiros de informações pessoais.

e. Situações em que o acesso pode ser limitado

i. Uma vez que as organizações devem sempre, de boa-fé, envidar todos os esforços para conceder o acesso dos cidadãos aos seus dados pessoais, as circunstâncias nas quais as organizações podem limitar tal acesso são limitadas e quaisquer razões apresentadas para justificar a recusa devem ser específicas. Tal como ao abrigo da diretiva, uma organização pode restringir o acesso a informações, sempre que a divulgação seja passível de interferir com a salvaguarda de interesses públicos igualmente importantes, nomeadamente a segurança nacional; a defesa; ou a segurança pública. Além disso, o acesso pode ser recusado quando a informação pessoal é tratada apenas para fins estatísticos ou de investigação. Outras razões para recusar ou limitar o acesso:

1. Interferência com a execução ou o cumprimento da lei ou com ações particulares, incluindo a prevenção, investigação ou deteção de delitos ou o direito a um processo equitativo;

2. Divulgação que viole os legítimos direitos ou interesses importantes de terceiros;

3. Quebra de uma obrigação ou privilégio de caráter jurídico ou profissional;

4. Prejuízo de investigações no âmbito da segurança dos trabalhadores ou de procedimentos de resolução de queixas ou para a planificação da sucessão dos trabalhadores e as reorganizações das empresas; ou

5. Prejuízo da confidencialidade necessária em matéria de acompanhamento, inspeções ou funções de regulamentação relativas a uma boa gestão, ou em negociações futuras ou em curso que impliquem a organização.

ii. Cabe à organização que invoca a exceção demonstrar a sua necessidade, bem como as razões de restrição do acesso e indicar um ponto de contacto para a obtenção de mais esclarecimentos às pessoas que o solicitem.

f. Direito de obter confirmação e cobrar uma taxa a fim de cobrir os encargos de acesso

i. Um cidadão tem o direito de obter a confirmação sobre se esta organização mantém dados pessoais sobre si. Um cidadão também tem o direito de lhe serem comunicados os dados pessoais sobre si. Uma organização pode cobrar uma taxa que não seja excessiva.

ii. A cobrança de uma taxa poderá ser justificada, por exemplo, sempre que os pedidos de acesso sejam manifestamente excessivos, nomeadamente devido ao seu caráter repetitivo.

iii. O acesso não pode ser recusado por razões relacionadas com os custos se a pessoa em causa se propuser pagá-los.

g. Pedidos de acesso repetidos ou abusivos

As organizações podem determinar limites razoáveis relativos ao número de vezes que, durante um dado período, se dará resposta aos pedidos de uma determinada pessoa. Ao definir estas limitações, uma organização deverá considerar determinados fatores, como, por exemplo, a frequência das atualizações da informação, a finalidade da utilização dos dados e a natureza da informação.

h. Pedidos de acesso fraudulentos

Uma organização não é obrigada a garantir o acesso à informação se não lhe forem fornecidos dados suficientes que lhe permitam confirmar a identidade da pessoa que efetua o pedido.

i. Prazo para a apresentação de respostas

As organizações devem dar resposta aos pedidos de acesso dentro de um prazo razoável, de forma razoável, e num formato facilmente inteligível para o cidadão. As organizações que forneçam, regularmente, informações aos titulares de dados poderão responder a um pedido de acesso individual com a sua divulgação periódica se tal não constituir um atraso excessivo.

9. **Dados relativos a recursos humanos**

a. Abrangência pelo Escudo de Proteção da Privacidade

i. Quando uma organização da UE transfere dados pessoais relativos aos seus trabalhadores (anteriores ou atuais), recolhidos no âmbito da relação de trabalho, para uma empresa-mãe, uma entidade associada ou um fornecedor de serviços não associado nos Estados Unidos que tenha aderido ao Escudo de Proteção da Privacidade, a transferência goza das condições por este garantidas. Nestes casos, a recolha de informação e o seu tratamento antes de efetuada a transferência deverão estar sujeitos à legislação nacional do país da UE onde se processou a recolha, bem como às condições ou restrições impostas à transferência que serão respeitadas de acordo com essa mesma legislação.

ii. Os princípios do Escudo de Proteção da Privacidade são pertinentes apenas no caso da transferência ou do acesso a registos individualmente identificados ou identificáveis. As estatísticas baseadas em dados agregados sobre o emprego sem dados pessoais ou a utilização de dados anónimos não levantam quaisquer preocupações em matéria de privacidade.

b. Aplicação dos princípios de aviso e escolha

i. Uma organização norte-americana que receba informações abrangidas pelo Escudo de Proteção da Privacidade, provenientes da UE, relativas a trabalhadores, só poderá divulgá-las a terceiros ou utilizá-las de forma diversa dos objetivos que presidiram à recolha inicial, em conformidade com os princípios de aviso e de escolha. Por exemplo, se uma organização pretender utilizar informações pessoais inicialmente recolhidas no âmbito de relações de trabalho para fins alheios à relação de trabalho, tais como, para fins de comunicações de *marketing*, a organização norte-americana deve, antes de mais, garantir às pessoas em causa o direito de escolha necessário, a não ser que estas tenham já autorizado o uso da informação para tais fins. Essa utilização não deve ser incompatível com os fins para os quais os dados pessoais foram recolhidos ou ulteriormente autorizados pela pessoa em causa. Além disso, qualquer escolha efetuada pelo trabalhador não poderá ser utilizada para limitar as oportunidades de emprego ou aplicar sanções ao referido trabalhador.

ii. Note-se que certas condições gerais aplicáveis às transferências a partir de determinados Estados-Membros da UE podem excluir o uso da informação para diferentes finalidades, mesmo após efetuada a sua transferência para fora da UE; nesses casos, as referidas condições terão de ser respeitadas.

iii. Acrescente-se que os empregadores devem envidar esforços razoáveis no sentido de respeitar as opções dos trabalhadores em matéria de privacidade, podendo, por exemplo, limitar o acesso aos dados pessoais, garantir o anonimato em relação a certos dados ou a atribuir códigos ou pseudónimos sempre que os nomes reais não sejam necessários para o objetivo de gestão em causa.

iv. A organização não aplicará os princípios de aviso e de escolha, na medida e durante o tempo que assim se justifique para não prejudicar a capacidade da organização em matéria de promoções, nomeações ou outras decisões de índole semelhante.

c. Aplicação do princípio de acesso

O princípio suplementar relativo ao acesso fornece orientações sobre os motivos que podem justificar a recusa ou limitação do acesso solicitado no contexto dos recursos humanos. É evidente que os empregadores da UE devem agir em conformidade com os regulamentos locais e assegurar que os trabalhadores da UE tenham acesso à informação nos moldes exigidos pela legislação dos seus países de origem, independentemente do local onde se tratam ou arquivam os dados. O Escudo de Proteção da Privacidade exige a colaboração da organização responsável pelo tratamento destes dados nos Estados Unidos, a qual deverá garantir o acesso, quer diretamente, quer através do empregador da UE.

d. Aplicação

i. Quando a informação pessoal for exclusivamente utilizada no âmbito das relações de trabalho, a organização na UE será a principal responsável pelos dados perante o trabalhador. Por esse motivo, sempre que os trabalhadores europeus apresentem uma queixa relativa à violação dos seus direitos em matéria de proteção dos dados e não estiverem satisfeitos com os resultados dos processos de verificação interna, queixa e recurso (ou com qualquer outro procedimento de resolução de queixas no âmbito de um contrato com um sindicato), deverão ser aconselhados a dirigir-se às entidades nacionais responsáveis pela proteção dos dados ou à autoridade laboral da jurisdição onde trabalham. Também se incluem aqui os casos em que a alegada utilização incorreta dos seus dados pessoais seja da responsabilidade da organização norte-americana que recebeu os dados fornecidos pelo empregador e implique, por conseguinte, uma alegada violação dos princípios do Escudo de Proteção da Privacidade. Esta será a forma mais eficaz de abordar os direitos e obrigações, que muitas vezes se sobrepõem, impostos pelas convenções, pela legislação local do trabalho e pela legislação relativa à proteção dos dados.

ii. Uma organização norte-americana aderente ao Escudo de Proteção da Privacidade que utilize os dados relativos aos recursos humanos da UE transferidos da União Europeia, no âmbito das relações de trabalho, e que pretenda que tais transferências sejam abrangidas pelo Escudo de Proteção da Privacidade tem, por conseguinte, de se comprometer a colaborar em qualquer investigação e a agir em conformidade com as orientações das autoridades comunitárias competentes na matéria.

e. Aplicação do princípio de responsabilização pela transferência ulterior

No que diz respeito a necessidades operacionais ocasionais relacionadas com o emprego das organizações aderentes ao Escudo de Proteção da Privacidade no que se refere aos dados pessoais transferidos ao abrigo deste, tais como a reserva de um voo, de um quarto de hotel ou a cobertura de seguro, as transferências de dados pessoais de um número reduzido de trabalhadores podem ser efetuadas para responsáveis pelo tratamento de dados sem a aplicação do princípio de acesso ou a celebração de um contrato com o terceiro responsável pelo tratamento dos dados, tal como de outro modo exigido pelo princípio de responsabilidade pela transferência ulterior, desde que a organização aderente ao referido quadro tenha respeitado os princípios de aviso e escolha.

10. **Contratos obrigatórios para transferências ulteriores**

a. Contratos de tratamento de dados

i. Quando os dados pessoais são transferidos da UE para os EUA com o objetivo exclusivo do seu tratamento (subcontratação), será necessário um contrato, independentemente da participação do subcontratante no Escudo de Proteção da Privacidade.

ii. Na Europa, os responsáveis pelo tratamento de dados são sempre obrigados a celebrar um contrato quando se efetua uma transferência para tratamento (subcontratação), seja esta processada no interior ou no exterior da UE e independentemente de o responsável pelo tratamento participar no Escudo de Proteção da Privacidade. O objetivo do contrato consiste em garantir que o subcontratante:

1. Só age de acordo com instruções do responsável pelo tratamento;

2. Aplica medidas técnicas e organizativas adequadas a fim de proteger os dados pessoais contra a destruição acidental ou ilegal ou a perda, a alternação, o acesso ou a divulgação não autorizados acidentais e compreende se a transferência ulterior está autorizada; e

3. Tomando em consideração a natureza do tratamento, assiste o responsável pelo tratamento dos dados na resposta aos cidadãos que exerçam os seus direitos nos termos dos princípios.

iii. Visto que os participantes no Escudo de Proteção da Privacidade garantem proteção adequada, os contratos com os participantes celebrados para mero tratamento não exigem autorização prévia (ou essa autorização será automaticamente garantida pelos Estados-Membros da UE), contrariamente aos contratos com destinatários que não tenham aderido ao referido quadro ou que não apliquem outra modalidade de proteção adequada.

b. Transferências num grupo controlado de empresas ou entidades

Sempre que sejam transferidas informações pessoais entre dois responsáveis pelo tratamento de dados num grupo controlado de empresas ou entidades, nem sempre é necessário um contrato nos termos do princípio de responsabilidade pela transferência ulterior. Os responsáveis pelo tratamento dos dados num grupo controlado de empresas ou entidades podem basear estas transferências noutros instrumentos, tais como as regras vinculativas para empresas da UE ou outros instrumentos internos do grupo (por exemplo, programas de controlo e conformidade), que assegurem a continuidade da proteção das informações pessoais ao abrigo dos princípios. No caso destas transferências, a organização aderente ao Escudo de Proteção da Privacidade permanece responsável pelo cumprimento dos princípios.

c. Transferências entre responsáveis pelo tratamento de dados

No que diz respeito às transferências entre responsáveis pelo tratamento de dados, não é necessário que o destinatário responsável pelo tratamento dos dados seja uma organização participante no Escudo de Proteção da Privacidade nem que disponha de um mecanismo de recurso independente. A organização participante no Escudo de Proteção da privacidade deve celebrar um contrato com o terceiro que será o destinatário dos dados e responsável pelo tratamento dos mesmos que preveja o mesmo nível de proteção que se encontra disponível nos termos do referido quadro, não incluindo o requisito de que o terceiro deve ser uma organização aderente ao Escudo de Proteção da Privacidade ou de que deve dispor de um mecanismo de recurso independente, desde que disponibilize um mecanismo equivalente.

11. **Resolução de litígios e aplicação**

a. O princípio de recurso, aplicação e responsabilidade estabelece os requisitos de aplicação do Escudo de Proteção da Privacidade. O princípio suplementar sobre verificação estabelece como cumprir os requisitos da alínea a), subalínea ii), do princípio. O presente princípio suplementar aborda a alínea a), subalíneas i) e iii), que exigem mecanismos de recurso independentes. Esses mecanismos podem assumir formas diferentes, mas todos devem cumprir os requisitos do princípio de recurso, aplicação e responsabilidade. As organizações cumprem os requisitos das seguintes maneiras: i) aplicando programas do setor privado de proteção da privacidade que respeitem os princípios do Escudo de Proteção da Privacidade nas suas regras e que incluam mecanismos de aplicação efetivamente eficazes do tipo descrito no princípio de recurso, aplicação e responsabilidade; ii) obedecendo às regras estabelecidas por entidades de controlo legal ou regulamentar que prevejam o tratamento de queixas individuais e resolução de litígios; ou iii) comprometendo-se a cooperar com as autoridades de proteção dos dados da União Europeia ou os seus representantes autorizados.

b. Esta lista pretende ser ilustrativa sem ser limitativa. O setor privado pode criar mecanismos adicionais de aplicação, desde que os mesmos cumpram o estabelecido no princípio de recurso, aplicação e responsabilidade e nos princípios suplementares. É de referir que os requisitos do princípio de recurso, aplicação e responsabilidade

complementam o requisito segundo o qual as iniciativas de autorregulamentação devem ser vinculativas, em conformidade com a secção 5 da *Federal Trade Commission Act*, que proíbe atos desleais e desonestos ou regulamentação ou legislação semelhante que proíba tais atos.

c. A fim de contribuir para assegurar o cumprimento dos seus compromissos relativos ao Escudo de Proteção da Privacidade e apoiar a administração do programa, as organizações, bem como os respetivos mecanismos de recurso independentes, devem apresentar informações relacionadas com o Escudo de Proteção da Privacidade sempre que estas sejam solicitadas pelo *Department of Commerce*. Além disso, as organizações devem responder com celeridade às queixas relativas à sua conformidade com os princípios transmitidas através do *Department of Commerce* pelas APD. A resposta deve indicar se a queixa tem méritos e, em caso positivo, as medidas que a organização aplicará para retificar o problema. O *Department of Commerce* protegerá a confidencialidade das informações que receber em conformidade com o direito dos EUA.

d. Mecanismos de recurso

i. Antes de mais, as pessoas devem ser encorajadas a apresentar queixas que possam ter à organização em causa, antes de recorrerem a mecanismos de recurso independentes. As organizações devem responder aos consumidores no prazo de 45 dias após a receção de uma queixa. A independência de um mecanismo de recurso é um dado factual que pode ser demonstrado, nomeadamente, através da imparcialidade, da transparência da composição e do financiamento, bem como de antecedentes meritórios comprovados. Como exigido pelo princípio de recurso, aplicação e responsabilidade, o recurso colocado à disposição das pessoas deve ser de fácil utilização e gratuito. Os organismos para a resolução de litígios devem investigar cada uma das queixas apresentadas pelas pessoas, a menos que se trate de queixas infundadas ou abusivas, o que não impedirá que a organização que gere o mecanismo de recurso estabeleça requisitos de elegibilidade; todavia, tais requisitos deverão ser transparentes e justificados (por exemplo, para excluir queixas que não se inserem no âmbito do programa ou que devam ser analisadas noutras instâncias), sem pôr em causa o compromisso de analisar queixas legítimas. Ademais, os mecanismos de recurso devem facultar às pessoas, no momento em que apresentam a respetiva queixa, informação completa e prontamente disponível sobre o funcionamento do mecanismo de resolução de litígios. A informação deverá incluir indicações sobre as práticas desse mecanismo em matéria de privacidade, em conformidade com os princípios do Escudo de Proteção da Privacidade. Deverão também cooperar no desenvolvimento de novos instrumentos, como formulários-tipo para a apresentação de queixas, que facilitem o procedimento de resolução de litígios.

ii. Os mecanismos de recurso independentes devem incluir nos seus sítios Web públicos informações sobre os princípios do Escudo de Proteção da Privacidade, bem como os serviços que prestam no seu âmbito. Estas informações devem incluir: 1) informações sobre os requisitos dos princípios do Escudo de Proteção da Privacidade em matéria de mecanismos de recurso independentes ou uma ligação para os mesmos; 2) uma ligação para o sítio Web do *Department of Commerce* relativo ao Escudo de Proteção da Privacidade; 3) um esclarecimento de que os seus serviços de resolução de litígios ao abrigo do Escudo de Proteção da Privacidade são gratuitos para os cidadãos; 4) uma descrição de como é possível apresentar uma queixa relacionada com o Escudo de Proteção da Privacidade; 5) o prazo para o tratamento das queixas relacionadas com o Escudo de Proteção da Privacidade; e 6), uma descrição do conjunto de possíveis vias de recurso.

iii. Os mecanismos de recurso independentes devem publicar um relatório anual que apresente estatísticas agregadas sobre os seus serviços de resolução de litígios. O relatório anual deve incluir o seguinte: 1) o número total de queixas relacionadas com o Escudo de Proteção da Privacidade recebidas durante o ano de referência; 2) os tipos de queixas recebidas; 3) as medidas de qualidade da resolução de litígios, tais como o período necessário para o tratamento da queixa; e 4), os resultados das queixas recebidas, designadamente o número e os tipos de reparações ou sanções aplicadas.

iv. Tal como estabelecido no anexo I, encontra-se disponível uma opção de arbitragem que possibilita ao cidadão determinar, no que se refere a queixas não resolvidas, se uma organização aderente ao Escudo de Proteção da Privacidade violou as suas obrigações nos termos dos princípios para com o cidadão, e se tal violação continua total ou parcialmente por resolver. Esta opção encontra-se disponível apenas para estes efeitos. Esta opção não se encontra disponível, por exemplo, no que se refere às derrogações aos princípios ([1]) ou no respeitante a uma alegação sobre a adequação do Escudo de Proteção da Privacidade. Ao abrigo desta opção de arbitragem, o Comité do Escudo de Proteção da Privacidade (constituído por um ou três árbitros, conforme o acordado pelas partes) têm competência para aplicar medidas equitativas, não monetárias e específicas do cidadão (tais como acesso, correção, eliminação ou devolução dos dados do cidadão em questão) necessárias para corrigir a violação dos princípios apenas no que se refere ao cidadão. Os cidadãos e as organizações aderentes ao Escudo de Proteção da Privacidade poderão solicitar o controlo jurisdicional e a execução de decisões de arbitragem nos termos da legislação dos EUA ao abrigo da *Federal Arbitration Act* (lei relativa à arbitragem federal).

([1]) Secção I, ponto 5, dos princípios.

e. Reparação e sanções

O resultado de quaisquer reparações decididas pelo organismo para a resolução de litígios deve ser de molde a garantir que os efeitos do incumprimento sejam anulados ou corrigidos pela organização, na medida do possível, e que, no futuro, a organização proceda em conformidade com os princípios, podendo mesmo, se tal for oportuno, deixar de processar os dados da pessoa que apresentou queixa. As sanções devem ser suficientemente rigorosas para garantir que a organização se conforme aos princípios. Um conjunto de sanções de diferentes graus de severidade permitirá que os organismos para a resolução de litígios reajam adequadamente aos vários níveis de incumprimento. As sanções devem incluir tanto a publicação de casos de incumprimento como a supressão de dados, em determinadas circunstâncias ([1]). Outras sanções podem consistir na suspensão ou retirada de autorização, em compensações a pessoas que sofram perdas decorrentes de não conformidade e injunções. Os organismos de autorregulamentação e para a resolução de litígios do setor privado têm que informar, se for caso disso, os tribunais ou as entidades governamentais com competência na matéria, sempre que tenham conhecimento de violação das regras por parte das organizações aderentes ao Escudo de Proteção da Privacidade, bem como o *Department of Commerce*.

f. Atividade da FTC

A FTC comprometeu-se a examinar prioritariamente as queixas em matéria de incumprimento dos princípios trazidas por: i) organizações de autorregulamentação em matéria de privacidade e outros organismos independentes para a resolução de litígios; ii) Estados-Membros da UE; e iii) o *Department of Commerce*, para determinar se há violação da secção 5 da *Federal Trade Commission Act*, que proíbe os atos ou as práticas desleais ou enganosas. Se o FTC concluir que tem razão(ões) para considerar que a secção 5 foi violada, pode resolver o assunto procurando obter uma decisão administrativa para fazer cessar e proibir as práticas denunciadas ou através da apresentação de uma queixa a um tribunal federal distrital, que se tiver êxito pode resultar numa decisão do tribunal com o mesmo efeito. O que precede inclui falsas alegações de adesão aos princípios do Escudo de Proteção da Privacidade ou de participação no referido quadro por organizações que já não constam da lista do Escudo de Proteção da Privacidade ou que nunca autocertificaram a sua adesão ao *Department of Commerce*. A FTC pode obter sanções de caráter civil por violação de uma decisão desse tipo e pode intentar uma ação civil ou penal por violação de uma decisão do tribunal federal. A FTC informará o *Department of Commerce* de qualquer ação que empreender. O *Department of Commerce* encoraja outros organismos governamentais a informá-lo sobre as decisões judiciais deste tipo ou sobre quaisquer outras disposições relativas à adesão aos princípios do Escudo de Proteção da Privacidade.

g. Incumprimento persistente

i. Caso determinada organização persista em não cumprir os princípios, deixará de beneficiar do Escudo de Proteção da Privacidade. As organizações que tenham persistido em não cumprir os princípios serão suprimidas da lista do Escudo de Proteção da Privacidade pelo *Department of Commerce* e devem devolver ou eliminar as informações pessoais recebidas ao abrigo do referido quadro.

ii. O incumprimento permanente ocorre sempre que uma organização que tenha apresentado ao *Department of Commerce* a respetiva autocertificação recuse cumprir a decisão final de um organismo privado de autorregulamentação, de um organismo independente para a resolução de litígios ou de uma entidade pública, ou que um desses organismos constate que uma organização desrespeita frequentemente os princípios, a ponto de o seu empenho no cumprimento dos princípios deixar de ser credível. Nestes casos, a organização deve informar imediatamente o *Department of Commerce*desses factos. Se não o fizer sujeitar-se-á a processo judicial ao abrigo da *False Statements Act* (18 U.S.C. § 1001). O abandono por parte de uma organização de um programa de autorregulamentação de proteção da privacidade do setor privado ou de um mecanismo independente de resolução de litígios não a isenta da sua obrigação de respeitar os princípios e constituiria um incumprimento persistente.

iii. O *Department of Commerce* suprimirá uma organização da lista do Escudo de Proteção da Privacidade em resposta a todas as informações relativas ao incumprimento persistente, quer provenham da própria organização, de um organismo de autorregulação em matéria de proteção da privacidade, de outro organismo independente de resolução de litígios ou de uma entidade pública; contudo, só poderá fazê-lo

([1]) Os organismos para a resolução de litígios têm poder discricionário no que se refere às circunstâncias em que aplicam estas sanções. Um dos fatores a considerar quando se toma a decisão de suprimir ou não os dados é o caráter sensível dos mesmos; deverá tomar-se também em consideração se a organização recolheu, utilizou ou divulgou informações em infração flagrante aos princípios do Escudo de Proteção da Privacidade.

após ter dado um prazo de 30 dias e uma oportunidade de resposta à organização em falta. De igual modo, a lista do Escudo de Proteção da Privacidade do *Department of Commerce* indicará claramente quais as organizações que beneficiam do quadro e as que dele deixaram de beneficiar.

iv. Uma organização que pretenda participar num organismo de autorregulamentação, com o objetivo de voltar a aderir ao Escudo de Proteção da Privacidade, deverá facultar a esse organismo todas as informações referentes à sua participação anterior no referido quadro.

12. **Prazo da opção de não participação**

a. Em geral, o objetivo do princípio de escolha é o de assegurar que as informações pessoais sejam utilizadas e divulgadas de uma forma compatível com as expectativas e opções da pessoa em causa. Por conseguinte, uma pessoa deve poder exercer em qualquer altura a opção de não participação, no que diz respeito à utilização de informações pessoais para fins de *marketing* direto, respeitando, contudo, quaisquer prazos razoáveis estabelecidos pela organização, para que esta disponha de tempo para aplicar a dita opção. Uma organização poderá também exigir informação suficiente que confirme a identidade da pessoa que solicita a não participação. Nos Estados Unidos, as pessoas podem exercer esta opção através de um programa central de não participação, como, por exemplo, o serviço de preferências no envio de publicidade pelo correio da associação de *marketing* direto (*Direct Marketing Association's Mail Preference Service*). As organizações que recorram a este serviço devem fomentar a respetiva utilização junto dos consumidores que não desejem receber informações comerciais. Em todo o caso, as pessoas deverão poder recorrer a mecanismos imediatamente disponíveis e pouco onerosos que lhes permitam o exercício desta opção.

b. Do mesmo modo, uma organização poderá utilizar informações para determinados fins de *marketing* direto, nos casos em que é impraticável dar à pessoa a oportunidade de optar pela não participação antes de utilizar a dita informação, desde que, imediatamente a seguir (ou em qualquer outra altura, mediante pedido), a organização garanta à pessoa a opção de recusar (sem qualquer encargo para ela) a receção de qualquer outra correspondência de *marketing* direto e atue em conformidade com os desejos dessa pessoa.

13. **Informação relacionada com viagens**

a. Pode transferir-se para organizações no exterior da UE a informação proveniente das reservas de bilhetes de avião e outras, relacionadas com viagens, por exemplo, a relativa a passageiros frequentes, a reservas em hotéis e necessidades especiais, como regimes alimentares impostos por razões religiosas ou assistência médica em várias ocasiões diferentes. De acordo com o artigo 26.º da diretiva, a transferência de dados pessoais «para um país terceiro que não assegure um nível de proteção adequado na aceção do n.º 2 do artigo 25.º» poderá ter lugar desde que: i) seja necessária para o fornecimento de serviços exigidos pelas pessoas, ou para a execução do acordo de «passageiro frequente», por exemplo, ou ii) a pessoa em causa tenha dado de forma inequívoca o seu consentimento à transferência. As organizações norte-americanas aderentes ao Escudo de Proteção da Privacidade asseguram uma proteção adequada dos dados pessoais, pelo que podem receber transferências de dados da UE, mesmo que não respeitem estas ou outras condições estabelecidas no artigo 26.º da diretiva. Dado que o Escudo de Proteção da Privacidade contém normas específicas em matéria de informações sensíveis, esse tipo de informação (que, por exemplo, poderá ter de ser obtido em virtude da necessidade de assistência médica da pessoa) poderá incluir-se nas transferências para as organizações aderentes. Em todo o caso, a organização que procede à transferência deve respeitar a legislação do Estado-Membro da UE onde se encontra, o qual poderá, nomeadamente, impor condições especiais de tratamento de dados sensíveis.

14. **Produtos farmacêuticos e medicinais**

a. Aplicação da legislação dos Estados-Membros da UE ou dos princípios do Escudo de Proteção da Privacidade

As leis dos Estados-Membros da UE aplicam-se à recolha de dados pessoais e a qualquer tratamento que tenha lugar antes da transferência para os EUA. Os princípios do Escudo de Proteção da Privacidade aplicam-se aos dados após a transferência para os EUA. Os dados utilizados para investigação farmacêutica e outros fins deveriam, se possível, ser anónimos.

b. Investigação científica futura

i. Os dados pessoais apurados em estudos de investigação médicos ou farmacêuticos específicos desempenham frequentemente um papel importante na investigação científica futura. Nos casos em que os dados pessoais recolhidos no âmbito de um estudo de investigação são transferidos para uma organização dos EUA aderente ao Escudo de Proteção da Privacidade, a mesma pode utilizá-los para uma nova atividade de investigação científica se os princípios de aviso e escolha tiverem sido apropriadamente respeitados desde o início. O aviso deve conter informação sobre quaisquer futuras utilizações específicas dos dados, como seguimentos periódicos, estudos conexos ou *marketing*.

ii. É compreensível que nem todas as utilizações futuras dos dados possam ser especificadas, dado que uma nova utilização para fins de investigação pode surgir de análises posteriores dos dados originais, de novas descobertas e progressos médicos, e de desenvolvimentos em matéria de regulamentação e de saúde pública. Se necessário, o aviso deve, por conseguinte, indicar que os dados pessoais podem futuramente ser utilizados em atividades não previstas de investigação médica e farmacêutica. Se essa utilização não for coerente com o (s) objetivo(s) geral(is) da investigação para a qual os dados pessoais foram originalmente recolhidos, ou à qual o indivíduo deu posteriormente o seu consentimento, deverá ser obtido um novo consentimento.

c. Retirada de um ensaio clínico

Os participantes podem a todo momento decidir retirar-se de um ensaio clínico, ou ser solicitados a fazê-lo. Quaisquer dados pessoais recolhidos antes da retirada podem ainda ser tratados juntamente com outros dados recolhidos no âmbito do ensaio clínico a condição que isso tenha sido esclarecido no aviso comunicado ao participante no momento em que o mesmo concordou participar.

d. Transferências para efeitos de regulamentação e supervisão

É permitido às empresas de dispositivos farmacêuticos e médicos fornecer dados pessoais provenientes de ensaios clínicos conduzidos na UE a reguladores nos Estados Unidos, para efeitos de regulamentação e supervisão. São permitidas transferências semelhantes a outras partes para além dos reguladores, como instalações de empresas e outros investigadores, em conformidade com os princípios de aviso e escolha.

e. Estudos «cegos»

i. Para garantir a objetividade, em muitos ensaios clínicos, os participantes — e, frequentemente, também os investigadores — não têm acesso a informação sobre o tratamento que cada participante está a receber. Autorizar esse acesso comprometeria a validade do estudo e dos resultados da investigação. Os participantes nesses ensaios clínicos (designados estudos «cegos») não têm de ter acesso aos dados relativos ao seu tratamento durante o ensaio, se essa limitação tiver sido explicada quando o mesmo aderiu ao ensaio; a divulgação dessa informação comprometeria a integridade do esforço de investigação.

ii. O assentimento em participar no ensaio nestas condições constitui já uma renúncia razoável ao direito de acesso. No seguimento da conclusão do ensaio e da análise dos resultados, os participantes devem poder ter acesso aos dados que lhes dizem respeito, se o solicitarem. Devem solicitá-los, em primeiro lugar, ao médico ou prestador de serviços de saúde de quem receberam tratamento no âmbito do ensaio clínico ou, em seguida, à organização patrocinadora.

f. Controlo da segurança e da eficácia do produto

Uma empresa de dispositivos farmacêuticos ou médicos não tem de aplicar os princípios do Escudo de Proteção da Privacidade no que diz respeito aos princípios de aviso, escolha, responsabilidade pela transferência ulterior e acesso nas suas atividades de controlo da segurança e da eficácia do produto, incluindo a notificação de episódios adversos e o rastreio dos pacientes/pessoas em causa que utilizam certos medicamentos ou

dispositivos médicos, desde que a adesão aos princípios não interfira com a observância dos requisitos regulamentares. Isto é válido tanto para as notificações efetuadas, por exemplo, pelos prestadores de cuidados de saúde às empresas de dispositivos farmacêuticos e médicos, como para as notificações efetuadas por estas empresas aos organismos governamentais como a *Food and Drug Administration*.

g. Dados codificados

Invariavelmente, os dados da investigação são codificados, na sua origem, com uma chave única pelo investigador principal, de modo a não revelar a identidade dos titulares de dados. As empresas farmacêuticas que patrocinam essa investigação não recebem a chave. O código original é conhecido apenas pelo investigador, pelo que apenas este pode identificar a pessoa em causa em circunstâncias especiais (por exemplo, quando é necessário um acompanhamento médico). Uma transferência de dados codificados desta forma, da UE para os EUA, não constituiria um caso de transferência de dados pessoais sujeita aos princípios do Escudo de Proteção da Privacidade.

15. **Registos públicos e informação disponível ao público**

a. As organizações devem aplicar os princípios de segurança, integridade dos dados e limitação da finalidade, bem como de recurso, aplicação e responsabilidade do Escudo de Proteção da Privacidade aos dados pessoais de fontes disponíveis ao público. Estes princípios são igualmente aplicáveis aos dados pessoais recolhidos de registos públicos, isto é, todos os arquivos conservados pelos organismos ou entidades estatais, a todos os níveis, que podem ser consultados pelo público em geral.

b. Não é necessário aplicar os princípios de aviso, escolha ou responsabilidade pela transferência ulterior à informação de registos públicos, se estes não estiverem combinados com informação não pública, e desde que se respeitem as condições de consulta estabelecidas pela jurisdição pertinente. Aliás, em geral, não é necessário aplicar os princípios de aviso, escolha ou responsabilidade pela transferência ulterior à informação disponível ao público, exceto se o responsável europeu da transferência indicar que tal informação é objeto de restrições que exigem a aplicação desses princípios pela organização que se propõe utilizá-la. As organizações não são responsáveis pela utilização dada à informação uma vez publicada.

c. Quando se verificar que uma organização divulgou intencionalmente informação pessoal em violação dos princípios, em benefício de si própria ou de terceiros, a sua participação deixará de ser aceite no Escudo de Proteção da Privacidade.

d. A aplicação dos princípios de acesso às informações de registos públicos não é necessária, desde que estas não estejam associadas a outras informações pessoais (exceto nos casos de uma quantidade mínima utilizada para catalogar ou organizar a informação desses registos); contudo, devem respeitar-se as condições de consulta exigidas pela respetiva instância de jurisdição. Em contrapartida, quando as informações dos registos públicos estão associadas a informações não provenientes de outros registos públicos, uma organização deve garantir o acesso a toda a informação, partindo do princípio de que esta não é objeto de outras exceções autorizadas.

e. À semelhança das informações obtidas a partir de registos públicos, não é necessário aplicar o princípio de acesso a informação que já seja disponibilizada ao grande público, desde que não esteja associada a informação não pública. As organizações especializadas na venda de informações acessíveis ao público podem responder ao pedido de acesso contra pagamento de uma taxa correspondente ao montante habitualmente cobrado pela organização. Alternativamente, as pessoas podem procurar obter a sua informação na primeira organização que originalmente reuniu os dados.

16. **Pedidos de acesso pelas autoridades públicas**

a. A fim de proporcionar transparência a respeito dos pedidos legítimos efetuados pelas autoridades públicas para obter o acesso a informações pessoais, as organizações aderentes ao Escudo de Proteção da Privacidade podem, a título voluntário, emitir relatórios de transparência periódicos sobre o número de pedidos de informações pessoais que recebem das autoridades públicas para o exercício de funções coercivas ou por motivos de segurança nacional, desde que tais comunicações estejam autorizadas nos termos da legislação aplicável.

b. As informações fornecidas pelas organizações aderentes ao Escudo de Proteção da Privacidade nestes relatórios, em conjunto com as informações divulgadas pelo setor das informações, a par de outras informações, podem contribuir para a reapreciação conjunta anual do funcionamento do Escudo de Proteção da Privacidade em conformidade com os princípios.

c. A ausência de aviso nos termos da alínea a), subalínea xii), do princípio de aviso não deve impedir ou prejudicar a capacidade de uma organização de responder aos pedidos legítimos.

Anexo I

Modelo de arbitragem

O presente anexo I apresenta as condições segundo as quais as organizações aderentes ao Escudo de Proteção da Privacidade são obrigadas a proceder à arbitragem de queixas, nos termos do princípio de recurso, aplicação e responsabilidade. A opção de arbitragem vinculativa descrita abaixo é aplicável a determinadas queixas «não resolvidas» relativas aos dados abrangidos pelo Escudo de Proteção da Privacidade UE-EUA. O objetivo desta opção consiste em oferecer um mecanismo célere, independente e equitativo, à escolha dos cidadãos, para a resolução de alegadas violações dos princípios não resolvidas por nenhum dos restantes mecanismos do Escudo de Proteção da Privacidade, se existentes.

A. **Âmbito de aplicação**

A presente opção de arbitragem encontra-se disponível para que os cidadãos determinem, no que se refere a queixas não resolvidas, se uma organização aderente ao Escudo de Proteção da Privacidade violou as suas obrigações nos termos dos princípios para com o cidadão em causa, e se tal violação continua total ou parcialmente por resolver. Esta opção encontra-se disponível apenas para estes efeitos. Esta opção não se encontra disponível, por exemplo, no que se refere às derrogações aos princípios ([1]) ou no respeitante a uma alegação sobre a adequação do Escudo de Proteção da Privacidade.

B. **Reparações disponíveis**

Ao abrigo desta opção de arbitragem, o Comité do Escudo de Proteção da Privacidade (constituído por um ou três árbitros, conforme o acordado pelas partes) têm competência para aplicar medidas equitativas, não monetárias e específicas do cidadão (tais como acesso, correção, eliminação ou devolução dos dados do cidadão em questão) necessárias para pôr remédio à violação dos princípios apenas no que se refere ao cidadão. Estes são os únicos poderes do comité de arbitragem no que diz respeito às reparações. Ao ponderar as reparações, o comité de arbitragem deve tomar em consideração outras reparações que já tinham sido aplicadas por outros mecanismos ao abrigo do Escudo de Proteção da Privacidade. Não se encontram disponíveis indemnizações, custos, taxas ou outras reparações. Cada parte suporta os honorários do próprio advogado.

C. **Requisitos prévios à arbitragem**

Um cidadão que decida invocar esta opção de arbitragem deve tomar as seguintes medidas antes de dar início a um pedido de arbitragem: 1) Expor a alegada violação diretamente à organização e conceder-lhe a oportunidade de resolver o problema no prazo estipulado na secção III, ponto 11, alínea d), subalínea i), dos princípios; 2) Utilizar o mecanismo de recurso independente ao abrigo dos princípios, que não acarreta custos para o indivíduo; e 3) Expor o problema através da sua autoridade responsável pela proteção dos dados ao *Department of Commerce* e permitir que este envide os seus melhores esforços para resolver o problema nos prazos estabelecidos na carta da *International Trade Administration* do *Department of Commerce*, sem custos para o cidadão.

A presente opção de arbitragem não pode ser invocada se a mesma alegada violação dos princípios apresentada pelo cidadão 1) tiver sido previamente objeto de arbitragem vinculativa; 2) tiver sido objeto de um acórdão final relativo a uma ação judicial da qual o cidadão fez parte; ou 3) tiver sido previamente objeto de um acordo entre as partes. Além disso, esta opção não pode ser invocada se uma autoridade responsável pela proteção dos dados da UE 1) tiver competência nos termos das secções III, ponto 5, ou III, ponto 9, dos princípios; ou 2) tiver competência para resolver a alegada violação diretamente junto da organização. A competência de uma APD para resolver a mesma queixa contra um responsável pelo tratamento de dados da UE não exclui, por si só, a invocação desta opção de arbitragem contra uma entidade jurídica diferente não vinculada pela autoridade da APD.

D. **Caráter vinculativo das decisões**

A decisão de um cidadão de invocar esta opção de arbitragem vinculativa é completamente voluntária. As decisões de arbitragem serão vinculativas para todas as partes na arbitragem. Depois de invocada, o cidadão abdica da opção de solicitar reparações pela mesma alegada violação noutro fórum, exceto que, se uma medida não monetária equitativa não resolver na íntegra a alegada violação, a invocação de arbitragem por parte do cidadão não exclui um pedido de indemnização disponível nos tribunais.

([1]) Secção I, ponto 5, dos princípios.

E. **Controlo e execução**

Os cidadãos e as organizações aderentes ao Escudo de Proteção da Privacidade poderão solicitar o controlo jurisdicional e a execução das decisões de arbitragem nos termos da legislação dos EUA ao abrigo da *Federal Arbitration Act* ([1]). Todos os casos deste tipo devem ser apresentados no tribunal federal distrital cuja abrangência territorial inclua o principal estabelecimento da organização aderente ao Escudo de Proteção da Privacidade.

Esta opção de arbitragem destina-se a resolver litígios individuais e as decisões de arbitragem não visam funcionar como um precedente persuasivo ou vinculativo em questões que envolvam outras partes, designadamente em arbitragens futuras ou nos tribunais da UE ou dos EUA, nem em processos da FTC.

F. **O comité de arbitragem**

As partes selecionarão os árbitros a partir da lista de árbitros discutida abaixo.

Em conformidade com a legislação aplicável, o *Department of Commerce* dos EUA e a Comissão Europeia desenvolverão uma lista de pelo menos 20 árbitros, selecionados com base na independência, na integridade e em competências especializadas. É aplicável o seguinte em relação a este processo:

Árbitros:

1) permanecerão na lista durante um período de três anos, na ausência de circunstâncias excecionais ou justa causa, renovável durante um período adicional de três anos;

2) não devem receber quaisquer instruções de, nem estar associados a, qualquer parte, qualquer organização aderente ao Escudo de Proteção da Privacidade, aos EUA, à UE, a qualquer Estado-Membro da UE nem a qualquer outra autoridade governamental, autoridade pública ou organismo de execução; e

3) devem estar habilitados a exercer Direito nos EUA e ser peritos na legislação norte-americana relativa a privacidade, bem como ser especializados na legislação da UE em matéria de proteção de dados.

G. **Procedimentos de arbitragem**

Em conformidade com a legislação aplicável, no prazo de seis meses a contar da adoção da decisão de adequação, o *Department of Commerce* e a Comissão Europeia concordarão em adotar um conjunto existente e estabelecido de procedimentos de arbitragem norte-americanos (por exemplo, das entidades AAA ou JAMS) para regular os processos perante o Comité do Escudo de Proteção da Privacidade, sob reserva de cada uma das seguintes considerações:

1. Um cidadão pode dar início a arbitragem vinculativa, sob reserva da disposição acima relativa aos requisitos prévios à arbitragem, através da apresentação de um «aviso» à organização. O aviso deve conter um resumo das medidas tomadas nos termos do ponto C para resolver a queixa, uma descrição da alegada violação e, à escolha do cidadão, quaisquer documentos e materiais comprovativos e/ou uma discussão da legislação relativa à alegada queixa.

([1]) O capítulo 2 da *Federal Arbitration Act* («FAA») prevê que «[u]m acordo de arbitragem ou uma sentença arbitral decorrentes de uma relação jurídica, contratual ou não, que seja considerada comercial, nomeadamente uma transação, um contrato ou acordo descritos na [secção 2 do FAA], são abrangidos pela Convenção [sobre o Reconhecimento e a Execução de Sentenças Arbitrais Estrangeiras de 10 de junho de 1958, 21 U.S.T. 2519, T.I.A.S. N.º 6997 («Convenção de Nova Iorque»)]». 9 U.S.C. § 202. Além disso, o FAA estabelece que «[d]eve considerar-se que um acordo ou sentença decorrente de uma relação desse tipo exclusivamente entre cidadãos dos Estados Unidos não é abrangido pela Convenção [de Nova Iorque], a menos que a relação implique imóveis localizados no estrangeiro, preveja o cumprimento ou a execução no estrangeiro, ou tenha alguma relação razoável de outro tipo com um ou mais Estados estrangeiros». *Id.* Nos termos do capítulo 2, «qualquer parte na arbitragem pode solicitar a qualquer tribunal com competência no âmbito do presente capítulo um acórdão que confirme a sentença como contra qualquer outra parte na arbitragem. O tribunal deve confirmar a sentença, a menos que constate um dos motivos de recusa ou diferimento do reconhecimento ou da execução da sentença especificados na referida Convenção [de Nova Iorque]». *Id.* § 207. Além disso, o capítulo 2 estipula que «[O]s tribunais distritais dos Estados Unidos […] devem ter competência original sobre […] uma ação ou um processo [nos termos da Convenção de Nova Iorque], independentemente do montante em questão». *Id.* § 203.
O capítulo 2 estabelece ainda que o «capítulo 1 é aplicável às ações e aos processos instaurados nos termos do presente capítulo, desde que o referido capítulo não seja contrário ao presente capítulo ou à Convenção [de Nova Iorque], tal como ratificada pelos Estados Unidos». *Id.* § 208. O capítulo 1, por sua vez, estabelece que «[u]ma disposição por escrito num […] contrato que evidencie uma transação que implique trocas comerciais para resolver por arbitragem uma controvérsia decorrente de tal contrato ou transação, ou a recusa em executar o mesmo parcialmente ou na íntegra, ou um acordo por escrito para submeter a arbitragem uma controvérsia exis»tente decorrente de um tal contrato, transação ou recusa, será válido, irrevogável e executório, salvo disposição em contrário na legislação ou nos tribunais para a revogação de qualquer contrato. *Id.* § 2. Além disso, o capítulo 1 estabelece que «qualquer parte na arbitragem pode solicitar ao tribunal assim especificado um acórdão que confirme a sentença e o tribunal deve emitir tal acórdão, a menos que a sentença seja abandonada, alterada ou corrigida, tal como prescrito nas secções 10 e 11 da [FAA]». *Id.* § 9.

2. Desenvolver-se-ão procedimentos para garantir que a mesma alegada violação de um cidadão não é alvo de reparações ou procedimentos duplicados.

3. A ação da FTC pode proceder em paralelo com a arbitragem.

4. Nenhuma autoridade representante dos EUA, da UE, de qualquer Estado-Membro da UE ou qualquer outra autoridade governamental, autoridade pública ou organismo de execução pode participar nestas arbitragens; contudo, mediante pedido de um cidadão da UE, as APD da UE podem prestar assistência na elaboração apenas do aviso, mas não podem ter acesso a conteúdos ou quaisquer outros materiais relacionados com estas arbitragens.

5. A arbitragem realizar-se-á nos Estados Unidos e o cidadão pode optar pela participação por videoconferência ou telefone, que será proporcionada sem custos para o cidadão. A participação em pessoa não será exigida.

6. A língua utilizada na arbitragem será o inglês, salvo acordo das partes em contrário. Mediante pedido fundamentado, e tomando em consideração se o cidadão é representado por um advogado, será fornecida interpretação na audição arbitral, bem como a tradução dos materiais de arbitragem, sem custos para o cidadão, a menos que o comité considere que, nas circunstâncias da arbitragem específica, tal conduziria a custos injustificados ou desproporcionados.

7. Os materiais apresentados aos árbitros serão tratados confidencialmente e serão utilizados apenas em relação à arbitragem.

8. Os conteúdos específicos do cidadão podem ser autorizados, se necessário, serão tratados confidencialmente pelas partes e serão utilizados apenas em relação à arbitragem.

9. A arbitragem deve ser concluída no prazo de 90 dias da apresentação do aviso à organização em questão, salvo acordo das partes em contrário.

H. **Custos**

Os árbitros devem tomar medidas razoáveis para minimizar os custos ou taxas das arbitragens.

Sob reserva da legislação aplicável, o *Department of Commerce* facilitará a instituição de um fundo, para o qual as organizações aderentes ao Escudo de Proteção da Privacidade serão obrigadas a pagar uma contribuição anual, baseada em parte na dimensão da organização, que abrangerá o custo de arbitragem, nomeadamente os honorários dos árbitros, até montantes máximos («limites»), em consulta com a Comissão Europeia. O fundo será gerido por um terceiro, que apresentará regularmente informações sobre o funcionamento do fundo. Na reapreciação anual, o *Department of Commerce* e a Comissão Europeia reapreciarão o funcionamento do fundo, designadamente a necessidade de ajustar o montante das contribuições ou dos limites e analisarão, entre outros elementos, o número de arbitragens, bem como os respetivos custos e calendarização, com o entendimento mútuo de que não será imposto um encargo financeiro excessivo sobre as organizações aderentes ao Escudo de Proteção da Privacidade. Os honorários dos advogados não são abrangidos pela presente disposição nem por qualquer fundo nos termos da presente disposição.

ANEXO III

Carta do Secretário de Estado dos EUA, John Kerry

7 de julho de 2016

Excelentíssima Senhora Comissária Vera Jourová,

Congratulo-me com o facto de termos chegado a acordo sobre o Escudo de Proteção da Privacidade União Europeia-Estados Unidos da América que incluirá um mecanismo de Mediador através do qual as autoridades na UE poderão apresentar pedidos em nome dos cidadãos da UE sobre as práticas dos EUA em matéria de informação de origem eletromagnética.

Em 17 de janeiro de 2014, o Presidente Barack Obama anunciou reformas importantes no domínio da informação que foram incluídas na *Presidential Policy Directive* 28 (PPD-28). Nos termos da PPD-28, nomeei a Subsecretária de Estado, Catherine A. Novelli, que ocupa igualmente o cargo de *Senior Coordinator for International Information Technology Diplomacy* (coordenadora superior da diplomacia internacional em matéria de tecnologia da informação), para exercer a função de ponto de contacto para os governos estrangeiros que desejem manifestar preocupações relativamente às atividades de informação de origem eletromagnética dos EUA. Com base nesta função, instituí um mecanismo de Mediador para o Escudo de Proteção da Privacidade em conformidade com as condições estabelecidas no anexo A, que foi entretanto atualizado desde a minha carta de 22 de fevereiro de 2016. Dei instruções à Subsecretária de Estado Novelli para que exerça esta função. A Subsecretária de Estado Novelli é independente do setor das informações dos EUA e responde diretamente perante mim.

Dei instruções ao meu pessoal para que dedique os recursos necessários para a implementação deste novo mecanismo do Mediador, e estou certo de que este constituirá um meio eficaz para resolver as preocupações dos cidadãos da UE.

Queira aceitar a expressão da minha mais elevada consideração,

John F. Kerry

Anexo A

Mecanismo do Mediador para o Escudo de Proteção da Privacidade UE-EUA Relativamente à informação de origem eletromagnética

Reconhecendo a importância do quadro do Escudo de Proteção da Privacidade UE-EUA, o presente memorando estabelece o processo de implementação de um novo mecanismo, em conformidade com a *Presidential Policy Directive 28* (PPD-28), no que se refere à informação de origem eletromagnética ([1]).

Em 17 de janeiro de 2014, o Presidente Obama proferiu um discurso no qual anunciou reformas importantes no domínio da informação. Nesse discurso, salientou que «[o]s nossos esforços contribuem para proteger não apenas a nossa nação, mas também os nossos amigos e aliados. Os nossos esforços só serão eficazes se os cidadãos comuns de outros países estiverem confiantes de que os Estados Unidos respeitam igualmente a sua privacidade». O Presidente Obama anunciou a emissão de uma nova diretiva presidencial — a PPD-28— para «prescrever exatamente o que fazemos e o que não fazemos, no que diz respeito à nossa vigilância no estrangeiro».

A secção 4, alínea d), da PPD-28 exige que o Secretário de Estado nomeie um «*Senior Coordinator for International Information Technology Diplomacy*» (coordenador superior) «para exercer a função de ponto de contacto para os governos estrangeiros que desejem manifestar preocupações relativamente às atividades de informação de origem eletromagnética realizadas pelos EUA\». A Subsecretária de Estado C. Novelli exerce a função de coordenadora superior desde janeiro de 2015.

O presente memorando descreve um novo mecanismo que a coordenadora superior seguirá a fim de facilitar o tratamento dos pedidos relacionados com o acesso para efeitos de segurança nacional aos dados transmitidos da UE para os EUA nos termos do Escudo de Proteção da Privacidade, de cláusulas contratuais-tipo, regras vinculativas para as empresas, «derrogações,» ([2]) ou «possíveis derrogações futuras,» ([3]) através de vias estabelecidas em conformidade com a legislação e política norte-americanas aplicáveis e a resposta aos referidos pedidos.

1. **O Mediador para o Escudo de Proteção da Privacidade.** A coordenadora superior exercerá a função de Mediador para o Escudo de Proteção da Privacidade e nomeará funcionários adicionais do *State Department*, conforme adequado, para assistir no seu exercício das responsabilidades pormenorizadas no presente memorando. (Em seguida designada «coordenadora» e todos os funcionários que exerçam tais funções serão denominados «Mediador para o Escudo de Proteção da Privacidade»). O Mediador para o Escudo de Proteção da Privacidade trabalhará em estreita colaboração com os funcionários adequados de outros departamentos e organismos responsáveis pelo tratamento de pedidos em conformidade com a legislação e política aplicáveis dos Estados Unidos. O Mediador é independente do setor das informações. O Mediador responde diretamente perante o Secretário de Estado, que assegurará que este desempenhe as suas funções de forma objetiva e isenta de influências indevidas que possa afetar a resposta a fornecer.

2. **Coordenação eficaz.** O Mediador para o Escudo de Proteção da Privacidade terá competências para utilizar e coordenar efetivamente esforços com os organismos de supervisão, descritos abaixo, a fim de assegurar que

([1]) Uma vez que a Decisão da Comissão sobre a adequação da proteção assegurada pelo Escudo de Proteção da Privacidade UE-EUA é aplicável à Islândia, ao Liechtenstein e à Noruega, o pacote do Escudo de Proteção da Privacidade abrangerá tanto a União Europeia como estes três países. Consequentemente, as remissões para a UE e os seus Estados-Membros devem ser entendidas como incluindo a Islândia, o Liechtenstein e a Noruega.

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

([3]) Neste contexto, entende-se por «possíveis derrogações futuras» uma transferência ou transferências comerciais que ocorrem numa das seguintes condições, desde que a condição constitua uma fundamentação legalmente admissível para a transferência de dados pessoais da UE para os EUA: a) O titular dos dados tiver explicitamente dado o seu consentimento à transferência prevista, após ter sido informado dos possíveis riscos de tais transferências para si próprio devido à falta de uma decisão de adequação e das garantias adequadas; ou b) A transferência for necessária para proteger interesses vitais do titular dos dados ou de outras pessoas, se esse titular estiver física ou legalmente incapaz de dar o seu consentimento; ou c) No caso de uma transferência para um país terceiro ou uma organização internacional e de que nenhuma das outras derrogações ou possíveis futuras derrogações for aplicável só puder ser efetuada se não for repetitiva, apenas disser respeito a um número limitado de titulares de dados, for necessária para efeitos de interesses legítimos visados pelo responsável pelo seu tratamento, desde que a tais interesses não se sobreponham os interesses ou os direitos e liberdades do titular dos dados, e o responsável pelo tratamento tiver ponderado todas as circunstâncias relativas à transferência de dados e, com base nessa avaliação, tiver apresentado garantias adequadas no que respeita à proteção de dados pessoais.

a resposta do Mediador aos pedidos do organismo responsável pela resolução das queixas dos cidadãos da UE se baseia nas informações necessárias. Quando o pedido disser respeito à compatibilidade de vigilância com a legislação dos EUA, o Mediador para o Escudo de Proteção da Privacidade poderá cooperar com um dos organismos de supervisão independentes com poderes de investigação.

a. O Mediador para o Escudo de Proteção da Privacidade trabalhará em estreita colaboração com os funcionários do governo dos Estados Unidos, nomeadamente com os organismos independentes de supervisão adequados, a fim de assegurar que os pedidos completos são tratados e resolvidos em conformidade com as leis e políticas aplicáveis. Em especial, o Mediador para o Escudo de Proteção da Privacidade terá competências para trabalhar em estreita colaboração com o *Office of the Director of National Intelligence* (Gabinete do Diretor dos Serviços Nacionais de Informações), o *Department of Justice* e outros departamentos e organismos envolvidos na segurança nacional dos Estados Unidos, conforme adequado, bem como com os inspetores-gerais, os agentes responsáveis pela execução da *Freedom of Information Act* (lei relativa à liberdade de informação) e os agentes responsáveis pela proteção da privacidade e das liberdades cívicas.

b. O governo dos Estados Unidos basear-se-á em mecanismos de coordenação e supervisão de questões de segurança nacional nos departamentos e organismos a fim de contribuir para assegurar que o Mediador para o Escudo de Proteção da Privacidade consegue responder na aceção da secção 4, alínea e), aos pedidos completos nos termos da secção 3, alínea b).

c. O Mediador para o Escudo de Proteção da Privacidade pode submeter questões relacionadas com pedidos à *Privacy and Civil Liberties Oversight Board* (comissão de controlo da privacidade e das liberdades cívicas) para apreciação.

3. **Apresentação de pedidos.**

a. Um pedido será inicialmente apresentado às autoridades de supervisão dos Estados-Membros competentes para a supervisão dos serviços de segurança nacionais e/ou do tratamento de dados pessoais pelas autoridades públicas. O pedido será apresentado ao Mediador por um organismo centralizado da UE (a seguir denominado em conjunto «organismo responsável pela resolução de queixas dos cidadãos da UE»).

b. O organismo responsável pela resolução de queixas dos cidadãos da UE assegurará, em conformidade com as seguintes ações, que o pedido se encontra completo:

i) Verificará a identidade do cidadão e que este age em próprio nome e não na qualidade de representante de uma organização governamental ou intergovernamental.

ii) Garantirá que o pedido é efetuado por escrito e que contém as seguintes informações básicas:

— todas as informações que constituem a base do pedido,

— a natureza das informações ou da reparação solicitada,

— as entidades do governo dos Estados Unidos que considera estarem envolvidas, se alguma, e

— as restantes medidas tomadas a fim de obter as informações ou reparações solicitadas, bem como a resposta recebida através dessas outras medidas.

iii) Verificará se o pedido diz respeito a dados que se acredite razoavelmente terem sido transferidos da UE para os Estados Unidos nos termos do Escudo de Proteção da Privacidade, de cláusulas contratuais-tipo, regras vinculativas para empresas, derrogações ou possíveis derrogações futuras.

iv) Procederá à determinação inicial de que o pedido não é infundado, abusivo, ou apresentado de má-fé.

c. A fim de ser considerado completo para efeitos de posterior tratamento pelo Mediador para o Escudo de Proteção da Privacidade nos termos do presente memorando, não é necessário que o pedido demonstre que o governo dos Estados Unidos acedeu efetivamente aos dados do requerente através de atividades de informação de origem eletromagnética.

4. **Compromissos de comunicação com o organismo responsável pela resolução de queixas dos cidadãos da UE.**

a. O Mediador para o Escudo de Proteção da Privacidade acusará a receção do pedido ao organismo responsável pela resolução da queixa do cidadão da UE em causa.

b. O Mediador para o Escudo de Proteção da Privacidade procederá a uma análise inicial a fim de verificar se o pedido se encontra completo nos termos da secção 3, alínea b). Se o Mediador para o Escudo de Proteção da Privacidade detetar alguma deficiência ou tiver questões relativamente ao preenchimento do pedido, esta procurará resolver as referidas preocupações junto do organismo responsável pela resolução da queixa do cidadão da UE em causa.

c. Se, a fim de facilitar o tratamento adequado do pedido, o Mediador para o Escudo de Proteção da Privacidade necessitar de informações adicionais sobre o pedido, ou se o cidadão que apresentou inicialmente o pedido tiver de tomar medidas adicionais, o Mediador para o Escudo de Proteção da Privacidade informará o organismo responsável pela resolução da queixa do cidadão da UE em causa deste facto.

d. O Mediador para o Escudo de Proteção da Privacidade rastreará o estado dos pedidos e comunicará informações atualizadas sempre que adequado ao organismo responsável pela resolução da queixa do cidadão da UE em causa.

e. Após o preenchimento de um pedido nos termos descritos na secção 3 do presente memorando, o Mediador para o Escudo de Proteção da Privacidade apresentará, em tempo útil, uma resposta adequada ao organismo responsável pela resolução da queixa do cidadão da UE em causa, sob reserva da obrigação constante de proteger a informação em conformidade com as leis e políticas aplicáveis. O Mediador para o Escudo de Proteção da Privacidade apresentará uma resposta ao organismo responsável pela resolução da queixa do cidadão da UE em causa confirmando i) que a queixa foi devidamente investigada, e ii) que a legislação, a regulamentação, os decretos executivos, as diretivas presidenciais e as políticas dos organismos que estabelecem as limitações e garantias descritas na carta do ODNI foram respeitados ou, em caso de incumprimento, que este foi corrigido. O Mediador para o Escudo de Proteção da Privacidade não confirmará nem desmentirá se o cidadão foi objeto de vigilância nem confirmará a reparação específica aplicada. Tal como explicado em maior pormenor na secção 5, os pedidos relacionados com a FOIA serão tratados conforme estabelecido na referida lei e na regulamentação aplicável.

f. O Mediador para o Escudo de Proteção da Privacidade comunicará diretamente com o organismo europeu para a resolução de queixas dos cidadãos da UE que, por sua vez, será responsável por comunicar com a pessoa que apresenta o pedido. Se as comunicações diretas fizerem parte de um dos processos subjacentes descritos abaixo, tais comunicações serão realizadas de acordo com os procedimentos existentes.

g. Os compromissos constantes do presente memorando não serão aplicáveis às queixas de caráter geral que alegam que o Escudo de Proteção da Privacidade UE-EUA é incompatível com os requisitos da União Europeia em matéria de proteção dos dados. Os compromissos constantes do presente memorando são assumidos com base no entendimento comum por parte da Comissão Europeia e do governo dos EUA de que, tomando em consideração o âmbito dos compromissos do presente mecanismo, podem surgir restrições de recursos, designadamente no que diz respeito aos pedidos relacionados com a *Freedom of Information Act* (FOIA). Caso o exercício das funções do Mediador para o Escudo de Proteção da Privacidade excedam restrições de recursos razoáveis e impeçam o cumprimento destes compromissos, o governo dos EUA debaterá com a Comissão Europeia possíveis alterações que possam ser adequadas para resolver a situação.

5. **Pedidos de informação.** Os pedidos de acesso aos registos do governo dos Estados Unidos podem ser apresentados e tratados nos termos da *Freedom of Information Act* (FOIA).

a. A FOIA proporciona um meio para que qualquer pessoa solicite o acesso à documentação existente dos organismos federais, independentemente da nacionalidade do requerente. Esta lei encontra-se codificada no *United States Code* em 5 U.S.C. § 552. A lei, em conjunto com informações adicionais sobre a FOIA, encontra-se disponível em www.FOIA.gov e http://www.justice.gov/oip/foia-resources. Cada organismo tem um *Chief FOIA Officer*, e apresentou informações no seu sítio Web público sobre como apresentar um pedido relacionado com a FOIA ao organismo. Os organismos dispõem de processos de consulta entre si sobre questões relacionadas com a FOIA que implicam documentação detida por outro organismo.

b. Para citar alguns exemplos:

i) O Office of the Director of National Intelligence (ODNI) criou o portal ODNI FOIA para o ODNI: http://www.dni.gov/index.php/about-this-site/foia. Este portal fornece informações sobre a apresentação de um pedido, a verificação do estado de um pedido existente, bem como o acesso a informações divulgadas e publicadas pelo ODNI nos termos da FOIA. O portal ODNI FOIA inclui ligações para outros sítios sítio Web sobre a FOIA de elementos do setor das informações: http://www.dni.gov/index.php/about-this-site/foia/other-ic-foia-sites.

ii) O *Office of Information Policy* (gabinete da política de informação) do *Department of Justice* apresenta informações abrangentes sobre a FOIA: http://www.justice.gov/oip. Tal inclui não apenas informações sobre a apresentação de um pedido ao abrigo da FOIA junto do *Department of Justice*, mas também faculta orientações ao governo dos Estados Unidos sobre a interpretação e aplicação dos requisitos da FOIA.

c. Nos termos da FOIA, o acesso a arquivos públicos é objeto de determinadas exceções enumeradas. Estas incluem limites ao acesso a informações de segurança nacional classificadas, informações pessoais de terceiros e informações relativas a investigações relacionadas com funções coercivas, e são comparáveis às limitações impostas por cada Estado-Membro da UE com a sua própria legislação em matéria de acesso à informação. Estas limitações são igualmente aplicáveis a cidadãos norte-americanos e de países terceiros.

d. Os litígios relativos à divulgação de documentação solicitada nos termos da FOIA podem ser objeto de recurso por via administrativa e posteriormente no tribunal federal. O tribunal deve tomar uma decisão *de novo* sobre se a documentação é devidamente retida, 5 U.S.C. § 552(a)(4)(B), e pode exigir que o governo conceda o acesso à documentação. Em alguns casos, os tribunais anularam decisões do governo de que a informação deve ser retida como classificada. Embora não se encontrem disponíveis indemnizações pecuniárias, os tribunais podem emitir uma decisão sobre os honorários do advogado.

6. **Pedidos de medidas suplementares.** Um pedido que alegue uma violação da lei ou outra má conduta será submetido ao organismo adequado do governo dos Estados Unidos, designadamente a organismos independentes de supervisão, com competência para investigar o respetivo pedido e resolver casos de incumprimento conforme descrito abaixo.

a. Os Inspetores Gerais são juridicamente independentes; dispõem de amplas competências para realizar investigações, auditorias e reapreciações de programas, nomeadamente no que se refere a fraude e abuso ou violação da lei; e podem recomendar medidas corretivas.

i) A *Inspector General Act* (Lei sobre os Inspetores Gerais) de 1978, com as alterações que lhe foram introduzidas, estabeleceu por lei os Inspetores Gerais federais como unidades independentes e objetivas na maioria dos organismos cujas funções consistem em combater o desperdício, a fraude e o abuso nos programas e operações dos respetivos organismos. Para tal, cada Inspetor Geral é responsável pela realização de auditorias e investigações relacionadas com os programas e operações do seu organismo. Além disso, os Inspetores Gerais proporcionam liderança e coordenação, recomendam políticas para atividades que visam promover a economia, a eficiência e a eficácia e impedem e detetam fraudes e abuso, nos programas e operações dos organismos.

ii) Cada elemento do setor das informações dispõe do seu próprio *Office of the Inspector General* (Gabinete do Inspetor-Geral) com responsabilidade pela supervisão das atividades de informações externas, entre outras questões. Vários relatórios dos inspetores-gerais sobre programas de informações foram divulgados publicamente.

iii) Para citar alguns exemplos:

— O *Office of the Inspector General of the Intelligence Community* (Gabinete do Inspetor-Geral do Setor das Informações — IC IG) foi criado nos termos da secção 405 da Intelligence Authorization Act of Fiscal Year 2010 — http://www.gpo.gov/fdsys/pkg/PLAW-111publ259/pdf/PLAW-111publ259.pdf. O IC IG é responsável pela realização de auditorias, investigações, inspeções e reapreciações a nível do setor das informações que identificam e resolvem deficiências, vulnerabilidades e riscos sistémicos transversais às missões dos serviços do setor das informações, com o objetivo de afetar positivamente as economias e eficiências a nível do setor das informações. O IC IG está autorizado a investigar queixas ou informações relativas a alegações de uma violação da lei, regra, regulamentação, desperdício, fraude, abuso de autoridade ou um perigo significativo ou específico para a saúde e segurança públicas em relação ao ODNI e/ou aos programas e atividades do setor das informações. O IC IG apresenta informações sobre o contacto direto consigo para efeitos de apresentação de um relatório: http://www.dni.gov/index.php/about-this-site/contact-the-ig.

— O *Office of the Inspector General* (OIG) no Department of Justice (DOJ) dos EUA — https://www.justice.gov — constitui uma entidade independente criada por lei cuja missão consiste em detetar e impedir situações de desperdício, fraude, abuso e má conduta nos programas e no pessoal do DOJ, bem como promover a economia e a eficiência nesses programas. O OIG investiga alegadas violações da legislação penal e civil por parte dos funcionários do DOJ e também procede a auditorias e inspeções aos programas do DOJ. O OIG tem competência para apreciar todas as queixas de má conduta contra os funcionários do *Department of Justice*, nomeadamente o *Federal Bureau of Investigation* (Gabinete Federal de Investigação); a *Drug Enforcement Administration*; o *Federal Bureau of Prisons*; o *U.S. Marshals Service*; o *Bureau of Alcohol, Tobacco, Firearms, and Explosives*; os *United States Attorneys Offices*; e funcionários que trabalham noutros gabinetes ou divisões do Department of Justice. (A única exceção é que as alegações de má conduta por parte de um advogado do *Department of Commerce* ou de pessoal responsável pela aplicação da lei que diga

respeito ao exercício da autoridade do advogado do *Department of Commerce* para investigar, participar em processos ou prestar aconselhamento jurídico são da responsabilidade do *Office of Professional Responsibility* do *Department of Commerce*). Além disso, a secção 1001 da *Patriot Act*, aprovada em 26 de outubro de 2001, estabelece que o inspetor-geral deve analisar as informações e receber as queixas que aleguem abusos dos direitos cívicos e das liberdades cívicas pelos funcionários do *Department of Justice*. O OIG mantém um sítio Web público — https://www.oig.justice.gov — que inclui uma linha telefónica direta para a apresentação de queixas — https://www.oig.justice.gov/hotline/index.htm.

b. Os organismos e entidades responsáveis pela proteção da privacidade e das liberdades cívicas do governo dos Estados Unidos também têm responsabilidades relevantes. Para citar alguns exemplos:

i) A secção 803 das Recomendações de Execução da Lei da Comissão de 11 de setembro de 2007, codificada no *United States Code* em 42 U.S.C. § 2000-ee1 institui agentes responsáveis pela proteção da privacidade e das liberdades cívicas em determinados departamentos e organismos (nomeadamente o *Department of State*, o *Department of Justice* e o ODNI). A secção 803 especifica que estes agentes responsáveis pela proteção da privacidade e das liberdades cívicas exercerão a função de principal conselheiro a fim de, entre outros, assegurar que tal departamento, organismo ou elemento dispõe de procedimentos adequados para resolver queixas de cidadãos que aleguem que tal departamento, organismo ou elemento violou a sua privacidade ou as suas liberdades cívicas.

ii) O *Civil Liberties and Privacy Office* (gabinete responsável pela proteção da privacidade e das liberdades cívicas) do ODNI é liderado pelo ODNI *Civil Liberties Protection Officer* (agente responsável pela proteção das liberdades cívicas), um cargo criado pela *National Security Act* (lei relativa à segurança nacional) de 1948, com as alterações que lhe foram introduzidas. As funções do CLPO do ODNI consistem em garantir que as políticas e os procedimentos dos elementos do setor das informações incluem proteções adequadas da privacidade e das liberdades cívicas, bem como analisar e investigar queixas que aleguem o abuso ou a violação das liberdades cívicas e da privacidade nos programas e atividades do ODNI. O CLPO do ODNI apresenta informações ao público no seu sítio Web, designadamente instruções para a apresentação de queixas: www.dni.gov/clpo. Se o CLPO do ODNI receber uma queixa relativa à privacidade ou às liberdades cívicas que implique programas e atividades do setor das informações, trabalhará em colaboração com outros elementos do setor das informações sobre como a referida queixa deve ser posteriormente tratada no setor das informações. Importa salientar que a *National Security Agency* (Agência Nacional de Segurança — NSA) também dispõe de um *Civil Liberties and Privacy Office*, que apresenta informações sobre as suas responsabilidades no seu sítio *web* — https://www.nsa.gov/civil_liberties/. Se as informações indicarem que um organismo se encontra em situação de incumprimento relativamente aos requisitos de privacidade (por exemplo, um requisito nos termos da secção 4 da PPD-28), estes dispõem de mecanismos conformidade para analisar e corrigir o incidente. Os organismos são obrigados a comunicar as situações de incumprimento nos termos da PPD-28 ao ODNI.

iii) O *Office of Privacy and Civil Liberties* (OPCL) do *Department of Justice* apoia os deveres e responsabilidades do *Chief Privacy and Civil Liberties Officer* (CPCLO) do *Department of Commerce*. A principal missão do OPCL consiste em proteger a privacidade e as liberdades cívicas dos cidadãos norte-americanos, através da análise, supervisão e coordenação das operações do *Department of Commerce* em matéria de privacidade. O OPCL presta aconselhamento jurídico e orientações aos componentes do Department; assegura o respeito da privacidade por parte do *Department of Commerce*, nomeadamente a conformidade com a *Privacy Act* de 1974 (lei em matéria de privacidade), as disposições da *E-Government Act* de 2002 (lei sobre a administração em linha) e da *Federal Information Security Management Act* (lei federal relativa à gestão da segurança da informação), bem como as diretivas relativas à política da administração emitidas na sequência das referidas leis; desenvolve e presta formação ao *Department of Commerce* em matéria de privacidade; assiste o CPCLO no desenvolvimento da política do *Department of Commerce* em matéria de privacidade; elabora relatórios relativos à privacidade a apresentar ao Presidente e ao Congresso; e revê as práticas de tratamento das informações do *Department of Commerce* a fim de garantir que tais práticas são coerentes com a proteção da privacidade e das liberdades cívicas. O OPCL apresenta informações ao público sobre as suas responsabilidades em http://www.justice.gov/opcl.

iv) De acordo com 42 U.S.C. § 2000ee et seq., a Privacy and Civil Liberties Oversight Board analisará i) as políticas e os procedimentos, bem como a respetiva aplicação, por parte dos departamentos, organismos e elementos do poder executivo no que se refere aos esforços envidados para a proteção da nação contra o terrorismo a fim de garantir que a privacidade e as liberdades cívicas são protegidas, e ii) outras medidas tomadas pelo poder executivo relacionadas com os referidos esforços a fim de determinar se tais medidas protegem devidamente a privacidade e as liberdades cívicas e são coerentes com a legislação, regulamentação e as políticas em vigor em matéria de privacidade e liberdades cívicas. Deve receber e rever relatórios e outras informações dos agentes responsáveis pela proteção da privacidade e das liberdades cívicas e, sempre que adequado, apresentar-lhes recomendações sobre as suas atividades. A secção 803 das Recomendações de Execução da Lei da Comissão de 11 de setembro de 2007, codificadas em 42 U.S.C. § 2000ee-1, estabelece que os agentes responsáveis pela proteção da privacidade e das liberdades cívicas de oito organismos federais (a saber, o Secretário da Defesa, o Secretário da Segurança Interna, o diretor dos serviços nacionais de

informações, e o diretor da Central Intelligence Agency), bem como qualquer organismo adicional nomeado pela PCLOB, devem apresentar-lhes relatórios periódicos, nomeadamente sobre o número, a natureza e a disposição das queixas recebidas pelo respetivo organismo por alegadas violações. A lei de habilitação da PCLOB estabelece que esta entidade deve receber estes relatórios e, sempre que adequado, fazer recomendações aos agentes responsáveis pela proteção da privacidade e das liberdades cívicas relativamente às suas atividades.

ANEXO IV

Carta da Presidente da Federal Trade Commission, Edith Ramirez

7 de julho de 2016

POR CORREIO ELETRÓNICO

Věra Jourová
Comissária para a Justiça, Consumidores e Igualdade de Género
Comissão Europeia
Rue de la Loi/Wetstraat 200
1049 Bruxelas
Bélgica

Excelentíssima Senhora Comissária Vera Jourová:

A *Federal Trade Commission* (FTC) dos Estados Unidos aprecia a oportunidade de descrever a sua aplicação do novo quadro do Escudo de Proteção da Privacidade UE-EUA («Escudo de Proteção da Privacidade» ou «quadro»). Acreditamos que o quadro desempenhará um papel crucial na promoção de transações comerciais que protejam a privacidade num mundo cada vez mais interligado. Permitirá que as empresas realizem operações importantes na economia global, assegurando ao mesmo tempo que os consumidores da UE dispõem de proteções importantes em matéria de privacidade. Há muito que a FTC assumiu o compromisso de proteger a privacidade através das fronteiras e dará prioridade à aplicação do novo quadro. Em seguida, explicamos o historial da FTC no que diz respeito à aplicação sólida da privacidade em termos gerais, nomeadamente a nossa aplicação do programa original de «porto seguro», bem como a abordagem da FTC à aplicação do novo quadro.

Em primeiro lugar, a FTC expressou publicamente o seu compromisso de aplicar o programa «porto seguro» em 2000. Nessa data, o presidente da FTC na altura, Robert Pitofsky, transmitiu uma carta à Comissão Europeia que descrevia o compromisso da FTC de aplicar decididamente os princípios da privacidade em «porto seguro». A FTC continuou a cumprir este compromisso em quase 40 medidas de execução, inúmeras investigações adicionais e cooperação com autoridades europeias específicas responsáveis pela proteção dos dados («APD da UE») em questões de interesse mútuo.

Após a Comissão Europeia ter expressado preocupações, em novembro de 2013, relativamente à administração e aplicação do programa «porto seguro», nós e o *Department of Commerce* dos EUA encetámos consultas com funcionários da Comissão Europeia a fim de explorar formas de o reforçar. Enquanto essas consultas se encontravam em curso, em 6 de outubro de 2015, o Tribunal de Justiça da União Europeia emitiu uma decisão no processo *Schrems* que, entre outras coisas, invalidou a decisão da Comissão Europeia sobre a adequação do programa «porto seguro». Na sequência da decisão, continuámos a trabalhar em estreita colaboração com o Department of Commerce e a Comissão Europeia num esforço para reforçar as proteções em matéria de privacidade asseguradas aos cidadãos da UE. O quadro do Escudo de Proteção da Privacidade é um resultado destas consultas em curso. Tal como se verificou com o programa «porto seguro» a FTC compromete-se a proceder à aplicação decidida do novo quadro. A presente carta recorda esse compromisso.

Designadamente, confirmamos o nosso compromisso em quatro domínios principais: 1) atribuição de prioridade às transmissões de queixas e investigações; 2) resolução de queixas relativas à participação falsa ou enganosa no Escudo de Proteção da Privacidade; 3) acompanhamento permanente de decisões; e 4) aumento da participação e aplicação da cooperação com as APD da UE. Em seguida, apresentamos informações pormenorizadas sobre cada um destes compromissos e antecedentes relevantes sobre o papel da FTC na proteção da privacidade dos consumidores e na aplicação do «porto seguro», bem como o panorama mais amplo em matéria de privacidade nos Estados Unidos ([1]).

I. ANTECEDENTES

A. **Trabalho político e proteção da privacidade pela FTC**

A FTC dispõe de amplas competências em matéria de execução civil para promover a proteção dos consumidores e a concorrência na esfera comercial. Como parte do seu mandato de proteção dos consumidores, a FTC aplica um amplo conjunto de leis de proteção da privacidade e da segurança dos dados dos consumidores. O direito primário aplicado

([1]) Apresentamos informações adicionais sobre as leis federais e estaduais em matéria de privacidade no apêndice A. Além disso, está disponível um resumo das nossas ações recentes em matéria de proteção da privacidade e da segurança no sítio Web da FTC: https://www.ftc.gov/reports/privacy-data-security-update-2015.

pela FTC, a *FTC Act* (lei relativa à Comissão reguladora do comércio federal), proíbe atos ou práticas «desleais» e «enganosos» relativos aos comércio ([1]). Uma declaração, omissão ou prática é enganosa se é significativa e suscetível de induzir em erro um consumidor razoável nessas circunstâncias ([2]).Um ato ou prática é desleal se causa, ou é suscetível de causar, danos substanciais que não possam ser facilmente evitados pelos consumidores e não sejam contrabalançados por benefícios compensatórios para os consumidores ou para a concorrência ([3]). A FTC aplica ainda leis seletivas que protegem as informações relativas a saúde, crédito ou outras questões financeiras, bem como informações de crianças em linha e emitiu regulamentação que dá cumprimento a cada uma dessas leis.

A competência da FTC ao abrigo da *FTC Act* é aplicável às questões «relativas ao comércio». A FTC não tem competência em questões de aplicação do direito penal nem de segurança nacional. Além disso, a FTC não pode atingir a maioria das restantes ações governamentais. Além disso, existem exceções à competência da FTC em matéria de atividades comerciais, nomeadamente no que se refere aos bancos, às companhias aéreas, à atividade de seguros e às atividades das empresas públicas de telecomunicações. A FTC também não tem competência no que se refere à maioria das organizações sem fins lucrativos, mas tem competência no respeitante a instituições de caridade falsas ou outras organizações sem fins lucrativos que têm efetivamente fins lucrativos. A FTC também tem competência no que diz respeito às organizações sem fins lucrativos que obtêm lucros para os seus membros com fins lucrativos, designadamente através da concessão de benefícios económicos significativos a esses membros ([4]). Em alguns casos, a competência da FTC é concomitante com a de outros organismos responsáveis pela aplicação da lei.

Desenvolvemos relações de trabalho sólidas com as autoridades federais e estaduais e trabalhamos em estreita colaboração a fim de coordenar investigações ou transmitir queixas sempre que adequado.

A função coerciva constitui o eixo central da abordagem da FTC à proteção da privacidade. Até à data, a FTC intentou mais de 500 ações de proteção da privacidade e segurança das informações dos consumidores. Este conjunto de ações abrange informações em linha e fora de linha e inclui medidas coercivas contra grandes e pequenas empresas, que alegam que não procederam à eliminação de forma devida de informações sensíveis sobre os consumidores, que não asseguraram a proteção das informações pessoais dos consumidores, rastrearam os consumidores em linha de forma enganosa, enviaram mensagens eletrónicas não desejadas (*spam*) aos consumidores, instalaram *software* espião (*spyware*) ou outro *software* mal intencionado (*malware*) nos computadores dos consumidores, violaram regras de proibição de contacto e outras regras de *telemarketing* e recolheram e partilharam indevidamente informações dos consumidores em dispositivos móveis. As medidas de execução da FTC — tanto no mundo físico como digital — enviam uma mensagem importante às empresas sobre a necessidade de proteger a privacidade dos consumidores.

A FTC procedeu igualmente a inúmeras iniciativas políticas destinadas a aumentar a privacidade dos consumidores que integram os seus esforços de aplicação. A FTC realizou seminários de formação e emitiu relatórios que recomendam melhores práticas destinadas a melhorar a privacidade no ecossistema móvel; aumentar a transparência do setor da corretagem de dados; maximizar os benefícios dos megadados, minimizando ao mesmo tempos os respetivos riscos, nomeadamente para os consumidores de baixo rendimento e insuficientemente servidos; e salientar as implicações em matéria de privacidade e segurança do reconhecimento facial e da Internet das coisas, entre outros domínios.

Além disso, a FTC procede à educação dos consumidores e das empresas com o objetivo de melhorar o impacto das suas iniciativas de desenvolvimento político e aplicação. A FTC utilizou vários instrumentos — publicações, recursos em linha, seminários de formação e redes sociais — para oferecer materiais didáticos sobre um vasto conjunto de temas, nomeadamente, aplicações móveis, privacidade das crianças e segurança dos dados. Mais recentemente, a Comissão lançou a sua iniciativa «Começar pela segurança», que inclui novas orientações para as empresas com base nos ensinamentos retirados dos casos relativos à segurança dos dados dos organismos, bem como uma série de seminários de formação no país. Além disso, há muito que a FTC é líder na educação dos consumidores sobre segurança informática básica. No ano passado, o nosso sítio Web *OnGuard Online* e o seu homólogo em língua espanhola, *Alerta en Línea*, receberam mais de 5 milhões de visualizações.

B. **Proteções jurídicas dos EUA que beneficiam os consumidores da UE**

O quadro funcionará no contexto do panorama mais amplo da privacidade nos EUA, que protege os consumidores da UE de várias formas.

([1]) 15 U.S.C. § 45, a).

([2]) Ver *FTC Policy Statement on Deception*, que figura em anexo a *Cliffdale Assocs., Inc.*, 103 F.T.C. 110, 174 (1984), disponível em https://www.ftc.gov/public-statements/1983/10/ftc-policy-statement-deception.

([3]) Ver 15 U.S.C § 45, n); *FTC Policy Statement on Unfairness*, que figura em anexo a *Int'l Harvester Co.*, 104 F.T.C. 949, 1070 (1984), disponível em https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness.

([4]) Ver *California Dental Ass'n* v. FTC, 526 U.S. 756 (1999).

A proibição da *FTC Act* relativa aos atos ou práticas desleais ou enganosos não se limita a proteger os consumidores norte-americanos das empresas dos EUA, uma vez que inclui as práticas que 1) causam, ou são suscetíveis de causar, danos razoavelmente previsíveis nos Estados Unidos ou 2) implicam uma conduta significativa nos Estados Unidos. Além disso, a FTC pode utilizar todas as reparações, nomeadamente a restituição, que se encontram disponíveis para proteger os consumidores nacionais quando protegem os consumidores estrangeiros.

Com efeito, o trabalho de aplicação da FTC beneficia significativamente tanto os consumidores norte-americanos como os estrangeiros. Por exemplo, os nossos casos que aplicam a secção 5 da *FTC Act* protegeram igualmente a privacidade dos consumidores norte-americanos e estrangeiros. Numa ação contra um corretor de informações, a Accusearch, a FTC alegou que a venda, por parte da empresa, de registos telefónicos confidenciais a terceiros sem o conhecimento ou o consentimento dos consumidores constituiu uma prática desleal em violação da secção 5 da *FTC Act*. A Accusearch vendeu informações relativas a consumidores norte-americanos e estrangeiros ([1]). O tribunal emitiu uma injunção contra a Accusearch que proíbe, entre outras coisas, a comercialização ou venda das informações pessoais dos consumidores sem o seu consentimento por escrito, a menos que estas tenham sido legitimamente obtidas de informações publicamente disponíveis e ordenou a restituição de quase 200 000 USD ([2]).

O acordo da FTC com a TRUSTe constitui outro exemplo. Assegura que os consumidores, nomeadamente os consumidores da União Europeia, podem confiar nas declarações apresentadas por uma organização global de autorregulamentação sobre a sua análise e certificação de serviços em linha nacionais e estrangeiros ([3]). Importa salientar que a nossa ação contra a TRUSTe reforça igualmente o sistema privado de autorregulamentação mais amplamente, assegurando a responsabilização das entidades que desempenham um papel importante nos regimes de autorregulamentação, designadamente nos quadros de privacidade estrangeiros.

Além disso, a FTC aplica outras leis seletivas cujas proteções são alargadas aos consumidores de países terceiros, tais como a *Children's Online Privacy Protection Act* (lei relativa à proteção da privacidade das crianças em linha — «COPPA»). Entre outras coisas, a COPPA exige que os operadores de sítios Web e serviços em linha orientados para crianças, ou sítios destinados ao público em geral que com conhecimento de causa recolhem informações pessoais de crianças com idade inferior a 13 anos, apresentem um aviso aos pais e obtenham o consentimento verificável dos mesmos. Os serviços e sítio Web sediados nos EUA que estão abrangidos pela COPPA e recolhem informações pessoais de crianças estrangeiras são obrigados a cumprir os disposto na COPPA. Os serviços em linha e sítios Web sediados no estrangeiro também devem respeitar a COPPA se forem orientados para crianças nos Estados Unidos ou se recolherem com conhecimento de causa informações pessoais de crianças nos Estados Unidos. Para além das leis federais dos EUA aplicadas pela FTC, determinadas outras leis federais e estaduais relativas à privacidade e à proteção do consumidor podem proporcionar benefícios adicionais aos consumidores da UE.

C. **Medidas coercivas no âmbito do «porto seguro»**

No âmbito do seu programa de proteção da privacidade e da segurança, a FTC também procurou proteger os consumidores da UE através de medidas coercivas relativas a violações do «porto seguro». A FTC interpôs 39 medidas coercivas no âmbito do «porto seguro»: 36 relativas a falsas alegações de certificação e três casos — contra Google, Facebook e Myspace — relativas a alegadas violações dos princípios da privacidade no âmbito do «porto seguro» ([4]). Estas casos demonstram a executoriedade das certificações e as repercussões do incumprimento. Injunções de vinte anos exigem que a Google, o Facebook e o Myspace implementem programas de proteção da privacidade abrangentes que devem ser razoavelmente concebidos para enfrentar os riscos para a privacidade relacionados com o desenvolvimento e a gestão dos produtos e serviços novos e existentes, bem como para proteger a privacidade e a confidencialidade das informações pessoais. Os programas de proteção da privacidade abrangentes mandatados nos termos destes despachos devem identificar riscos significativos previsíveis e dispor de controlos para fazer face a esses riscos. As empresas devem submeter-se igualmente a avaliações independentes contínuas dos seus programas de proteção da privacidade, que devem ser apresentadas à FTC. Além disso, os despachos proíbem que estas empresas prestem declarações falsas sobre as suas práticas em matéria de proteção da privacidade e a sua participação em qualquer programa de proteção da privacidade ou da segurança. Esta proibição seria igualmente aplicável aos atos e práticas das empresas no âmbito do

([1]) Ver *Office of the Privacy Commissioner of Canada, Complaint under PIPEDA against Accusearch, Inc., doing business as Abika.com*, https://www.priv.gc.ca/cf-dc/2009/2009_009_0731_e.asp. O *Office of the Privacy Commissioner* (Gabinete do Comissário responsável pela Proteção da Vida Privada) do Canadá apresentou um relatório de *amicus curiae* no recurso da ação da FTC e realizou a sua própria investigação, concluindo que as práticas da Accusearch também violaram a legislação do Canadá.

([2]) Ver *FTC v. Accusearch, Inc.*, n.º 06CV015D (D. Wyo. 20 de dezembro de 2007), *aff'd* 570 F.3d 1187 (10th Cir. 2009).

([3]) Ver *In the Matter of True Ultimate Standards Everywhere, Inc.*, n.º C-4512 (F.T.C. 12 de março de 2015) (decisão e despacho), *disponível em* https://www ftc.gov/system/files/documents/cases/150318trust-edo.pdf.

([4]) Ver *In the Matter of Google, Inc.*, n.º C-4336 (F.T.C. 13 de outubro de 2011) (decisão e despacho), *disponível em* https://www.ftc.gov/news-events/press-releases/2011/03/ftc-charges-deceptive-privacy-practices-googles-rollout-its-buzz; *In the Matter of Google, Inc.*, n.º C-4336 (F.T.C. 27 de julho de 2012) (decisão e despacho), *disponível em* https://www ftc.gov/news-events/press-releases/2012/08/ftc-approves-final-settlement-facebook; *In the Matter of Myspace LLC*, No. C-4369 (F.T.C. 30 de agosto de 2012) (decisão e despacho), *disponível em* https://www.ftc.gov/news- events/press-releases/2012/09/ftc-finalizes-privacy-settlement-myspace.

novo quadro do Escudo de Proteção da Privacidade. A FTC pode dar execução a estes despachos solicitando a aplicação de sanções de caráter civil. Com efeito, a Google pagou uma sanção de caráter civil com o valor recorde de 22,5 milhões de USD em 2012 para resolver alegações de que tinha violado o seu despacho. Consequentemente, estes despachos da FTC contribuem para proteger mais de mil milhões de consumidores a nível mundial, centenas de milhões dos quais residem na Europa.

As ações da FTC incidiram ainda sobre alegações falsas, enganosas ou deturpadas relativas à participação no «porto seguro». A FTC encara estas alegações com seriedade. Por exemplo, em *FTC/Karnani*, a FTC intentou uma ação em 2011 contra um comerciante na Internet nos Estados Unidos, alegando que este e a sua empresa induziram os consumidores britânicos em erro, levando-os a acreditar que a empresa se encontrava sediada no Reino Unido, nomeadamente através da utilização de extensões Web.uk, da menção à moeda britânica e ao sistema postal do Reino Unido ([1]). Todavia, quando os consumidores receberam os produtos, descobriram direitos de importação inesperados, garantias que não eram válidas no Reino Unido e taxas associadas à obtenção de reembolsos. Além disso, a FTC acusou os requeridos de induzirem os consumidores em erro relativamente à sua participação no programa «porto seguro». Nomeadamente, todos os consumidores que foram vítimas desta situação encontravam-se no Reino Unido.

Muitas das nossas restantes medidas coercivas no âmbito do «porto seguro» envolveram organizações que aderiram ao referido programa, mas que não renovaram a sua certificação anual tendo, no entanto, continuado a representar-se como membros atuais. Tal como discutido mais adiante, a FTC também se compromete a resolver as falsas alegações de participação no quadro do Escudo de Proteção da Privacidade. Esta atividade coerciva estratégica complementará o aumento das ações do *Department of Commerce* com o objetivo de verificar a conformidade com os requisitos do programa em matéria de certificação e de renovação da certificação, o seu controlo do cumprimento efetivo, designadamente através da utilização de questionários aos participantes no quadro, e o aumento dos seus esforços para identificar falsas alegações de participação no quadro e utilização indevida de qualquer marca de certificação do quadro ([2]).

II. ATRIBUIÇÃO DE PRIORIDADE ÀS QUEIXAS SUBMETIDAS E INVESTIGAÇÕES

Tal como realizado no programa «porto seguro», a FTC compromete-se a atribuir prioridade às queixas relativas ao Escudo de Proteção da Privacidade submetidas pelos Estados-Membros da UE. Além disso, atribuiremos prioridade às queixas de incumprimento de diretrizes de autorregulamentação relacionadas com o Escudo de Proteção da Privacidade de organizações de autorregulamentação em matéria de privacidade e de outros organismos independentes para a resolução de litígios.

Para facilitar a apresentação de queixas ao abrigo do quadro provenientes dos Estados-Membros da UE, a FTC está a criar um processo de transmissão de queixas normalizado e a fornecer orientações aos Estados-Membros da UE sobre o tipo de informações mais úteis para a instrução das queixas por parte da FTC. Como parte deste esforço, a FTC nomeará um ponto de contacto para o tratamento das queixas provenientes dos Estados Membros da UE. É vivamente recomendável que a autoridade que transmite a queixa tenha procedido a uma instrução preliminar da alegada violação e esteja em condições de cooperar com a FTC na eventualidade de uma investigação.

Após a receção de uma queixa proveniente de um Estado-Membro da UE ou de uma organização de autorregulamentação, a FTC pode tomar várias medidas para resolver os problemas em causa. Por exemplo, poderemos proceder à reapreciação das políticas da empresa em matéria de proteção da privacidade, obter informações adicionais diretamente da empresa ou de terceiros, proceder ao acompanhamento junto da entidade que submete a queixa, avaliar se existe um padrão de violações ou um número significativo de consumidores afetados, determinar se a queixa submetida implica questões da competência do *Department of Commerce*, estudar a utilidade de eventuais medidas de sensibilização dos consumidores e das empresas e, sempre que adequado, dar início a um processo coercivo.

A FTC compromete-se ainda a proceder ao intercâmbio de informações sobre as queixas com as autoridades responsáveis pelas medidas coercivas que apresentaram tais queixas, designadamente sobre o ponto da situação quanto as estas, sob reserva da leis e restrições em matéria de confidencialidade. Na medida do possível, tendo em conta o número e o tipo de queixas recebidas, as informações apresentadas incluirão uma avaliação dos elementos do processo, nomeadamente uma descrição de questões importantes levantadas e quaisquer medidas tomadas para corrigir as violações da lei no âmbito da competência da FTC. Além disso, a FTC transmitirá informações de retorno à

([1]) Ver *FTC v. Karnani*, N.º 2:09-cv-05276 (C.D. Cal. 20 de maio de 2011) (despacho final), *disponível em* https://www ftc.gov/sites/default/files/documents/cases/2011/06/110609karnanistip.pdf; *ver também* Lesley Fair, FTC Business Center Blog, *Around the World in Shady Ways*, http://www.business.ftc.gov/blog/2011/06/around-world-shady-ways (9 de junho de 2011).

([2]) Carta de Ken Hyatt, Subsecretário interino do Comércio, responsável pelo comércio internacional e a administração internacional do comércio, para Věra Jourová, Comissária da Justiça, Consumidores e Igualdade de género.

autoridade que submete a queixa sobre os tipos de queixas recebidos, a fim de aumentar a eficácia dos esforços no sentido de fazer face à conduta ilegal. Caso um organismo responsável pelas medidas coercivas solicite informações sobre o ponto da situação de uma queixa específica que tenha submetido para proceder à adoção de medidas coercivas, a FTC responderá, tomando em consideração o número de queixas em análise e sob reserva de requisitos de confidencialidade e outros requisitos jurídicos.

A FTC trabalhará ainda em estreita colaboração com as APD da UE com vista à prestação de assistência no domínio da execução de medidas coercivas. Consoante os casos, tal poderia incluir a partilha de informações e assistência na investigação nos termos da *Safe Web Act* (lei relativa à segurança da Web), que autoriza a assistência da FTC a organismos estrangeiros responsáveis pela aplicação de medidas coercivas sempre que estes organismos estrangeiros apliquem leis que proíbam práticas substancialmente semelhantes às proibidas pelas leis a que a FTC dá execução ([1]). No âmbito desta assistência, a FTC pode partilhar informações obtidas em relação a uma investigação da FTC, lançar um processo obrigatório em nome da APD da UE que realiza a sua própria investigação e solicitar o depoimento oral de testemunhas ou requeridos em relação ao processo de execução da APD, sob reserva dos requisitos previstos na *Safe Web Act*. A FTC utiliza regularmente este poder para assistir outros organismos em todo o mundo em processos relacionados com a proteção do consumidor e da privacidade ([2]).

Para além de atribuir prioridade às queixas relativas ao Escudo de Proteção da Privacidade submetidas pelos Estados-Membros da UE e por organizações de autorregulamentação em matéria de privacidade ([3]),a FTC compromete-se a investigar possíveis violações do quadro por iniciativa própria, sempre que adequado, utilizando vários instrumentos.

Durante mais de uma década, a FTC aplicou um programa sólido de investigação de questões relativas à proteção da privacidade e da segurança que envolvem organizações comerciais. No âmbito destas investigações, a FTC examinou sistematicamente se a entidade em questão apresentava declarações sobre o «porto seguro». Caso a entidade prestasse tais declarações e a investigação revelasse violações aparentes dos princípios da privacidade em «porto seguro», a FTC incluía alegações de violações do «porto seguro» nas suas medidas de execução. Continuaremos esta abordagem proativa no âmbito do novo quadro. Importa salientar que a FTC realiza muito mais investigações do que as que acabam por resultar em medidas de execução públicas. Muitas investigações da FTC são encerradas porque o pessoal não identifica nenhuma aparente violação da legislação. Uma vez que as investigações da FTC são de natureza não pública e confidencial, muitas vezes o encerramento de uma investigação não é tornado público.

As quase 40 medidas de execução iniciadas pela FTC relativas ao programa «porto seguro» evidenciam o compromisso do organismo no que se refere à execução proativa dos programas de proteção da privacidade estrangeiros. A FTC procurará potenciais violações do quadro no âmbito das investigações em matéria de proteção da privacidade e da segurança que realiza regularmente.

III. RESOLUÇÃO DE ALEGAÇÕES FALSAS OU ENGANOSAS DE PARTICIPAÇÃO NO ESCUDO DE PROTEÇÃO DA PRIVACIDADE

Tal como supramencionado, a FTC tomará medidas contra as entidades que prestem declarações falsas relativamente à sua participação no quadro. A FTC atribuirá prioridade à apreciação das queixas transmitidas pelo *Department of Commerce* sobre organizações que identifique que aleguem indevidamente ser membros atuais do quadro ou que utilizem qualquer marca de certificação sem autorização.

Além disso, salientamos que se a política de proteção da privacidade de uma organização promete que cumpre os princípios do Escudo de Proteção da Privacidade, a não efetuação ou manutenção de um registo junto do *Department of Commerce* provavelmente não irá, por si só, isentar a organização da execução desses compromissos do quadro por parte da FTC.

([1]) Ao determinar se deve ou não exercer as suas competências nos termos da *Safe Web Act*, a FTC analisa, nomeadamente: «a) Se o organismo requerente concordou em prestar ou prestará assistência recíproca à Comissão; b) se o cumprimento do pedido prejudicaria o interesse público dos Estados Unidos; e c) se a investigação ou o processo de aplicação de medidas coercivas do organismo requerente diz respeito a atos ou práticas que causam ou são suscetíveis de causar danos a um número significativo de pessoas.» 15 U.S.C. § 46(j)(3). Estas competências não dizem respeito à aplicação do direito da concorrência.

([2]) Nos exercícios financeiros de 2012 a 2015, por exemplo, a FTC utilizou as suas competências ao abrigo da *Safe Web Act* para partilhar informações em resposta a quase 60 pedidos de organismos estrangeiros e emitiu quase 60 decisões de investigação civil (equivalentes a intimações administrativas) para ajudar 25 investigações estrangeiras.

([3]) Embora a FTC não proceda à resolução ou mediação de queixas de consumidores individuais, a FTC confirma que atribuirá prioridade às queixas no âmbito do Escudo de Proteção da Privacidade submetidas pelas APD da UE. Além disso, a FTC utiliza queixas na sua base de dados *Consumer Sentinel*, que se encontra à disposição de muitos outros organismos responsáveis pela aplicação da lei, para identificar tendências, determinar prioridades em termos de execução e identificar potenciais alvos de investigação. Os cidadãos da UE podem utilizar o mesmo sistema de apresentação de queixas acessível aos cidadãos dos EUA para apresentar uma queixa à FTC em http://www.ftc.gov/complaint. Contudo, no que se refere às queixas individuais relativas ao Escudo de Proteção da Privacidade, pode ser mais útil para os cidadãos da UE apresentar queixas à APD ou à entidade de resolução alternativa de litígios do seu Estado-Membro.

IV. ACOMPANHAMENTO DE DESPACHOS

A FTC confirma ainda o seu compromisso de acompanhar os despachos de execução a fim de garantir a conformidade com o quadro do Escudo de Proteção da Privacidade.

Exigiremos a conformidade com o quadro através de várias disposições de injunção adequadas em futuros despachos da FTC relativos ao quadro. O que precede inclui a proibição de declarações fraudulentas relativas ao quadro e a outros programas de proteção da privacidade quando estes constituem a base da ação subjacente da FTC.

As ações da FTC que dão execução ao programa «porto seguro» original são elucidativas. Nas 36 ações que dizem respeito a alegações falsas ou enganosas de certificação no «porto seguro», cada despacho proíbe o requerido de prestar declarações fraudulentas sobre a sua participação no «porto seguro» ou em qualquer outro programa de proteção da privacidade ou da segurança e exige que a empresa disponibilize relatórios de conformidade à FTC. Nas ações relativas a violações dos princípios de privacidade em «porto seguro», as empresas foram obrigadas a implementar programas de proteção da privacidade abrangentes e a obter avaliações independentes desses programas efetuadas por terceiros de dois em dois anos durante 20 anos, que devem apresentar à FTC.

As violações dos despachos administrativos da FTC podem conduzir a sanções civis máximas de 16 000 USD por violação ou 16 000 USD por dia por uma violação contínua ([1]),que, no caso de práticas que afetam muitos consumidores, pode ascender a milhões de dólares norte-americanos. Cada injunção contém igualmente disposições de comunicação e conformidade. As entidades visadas pelo despacho devem conservar os documentos que demonstram a sua conformidade durante um número de anos especificado. Os despachos devem igualmente ser divulgados aos funcionários responsáveis por assegurar o seu cumprimento.

A FTC controla sistematicamente a conformidade com os despachos relativos ao «porto seguro», tal como faz com todos os seus despachos. A FTC encara a execução dos seus despachos em matéria de proteção da privacidade e da segurança dos dados com seriedade e interpõe ações de execução sempre que necessário. Por exemplo, como salientado acima, a Google pagou uma sanção penal de 22,5 milhões de USD para resolver alegações de que tinha violado o despacho da FTC. Importa mencionar que os despachos da FTC continuarão a proteger todos os consumidores a nível mundial que interajam com uma empresa, não apenas os consumidores que tenham apresentado queixas.

Por último, a FTC continuará a manter uma lista em linha das empresas que são objeto de despachos obtidos em relação à execução do programa «porto seguro» e do novo quadro do Escudo de Proteção da Privacidade ([2]). Além disso, os princípios do Escudo de Proteção da Privacidade exigem agora que as empresas objeto de uma decisão judicial ou da FTC por motivo de incumprimento dos referidos princípios devem publicar todas as partes inerentes ao Escudo de Proteção da Privacidade dos relatórios de conformidade ou de avaliação apresentados à FTC, limitadamente aos aspetos compatíveis com as leis e regulamentos em matéria de privacidade.

V. ENVOLVIMENTO COM AS APD DA UE E COOPERAÇÃO EM MATÉRIA DE EXECUÇÃO

A FTC reconhece o papel importante que as APD da UE desempenham no que se refere ao cumprimento do quadro e incentiva o aumento das consultas e da cooperação em matéria de execução. Para além das consultas com as APD que submetem queixas sobre questões específicas de determinadas ações, a FTC compromete-se a participar em reuniões periódicas com representantes designados do grupo de trabalho do artigo 29.º a fim de debater em termos gerais como melhorar a cooperação em matéria de execução no que diz respeito ao quadro. A FTC também participará, em conjunto com o *Department of Commerce*, a Comissão Europeia e representantes do grupo de trabalho do artigo 29.º, na reapreciação anual do quadro com o objetivo de debater a sua implementação.

A FTC promove ainda o desenvolvimento de instrumentos que melhorem a cooperação em matéria de execução com as APD da UE, bem como com outras autoridades responsáveis pela aplicação das leis relativas à proteção da privacidade em todo o mundo. Em especial, a FTC, em conjunto com parceiros de execução na União Europeia e em todo o mundo, lançou no último ano um sistema de alerta no âmbito da *Global Privacy Enforcement Network* («GPEN» — rede global para a proteção da vida privada) para a partilha de informações sobre investigações e a promoção da coordenação em matéria de execução. Este instrumento de alerta da GPEN poderia ser especialmente útil no contexto do quadro do Escudo de Proteção da Privacidade. A FTC e as APD da UE poderiam utilizá-lo para efeitos de coordenação no que diz respeito ao quadro e a outras investigações em matéria de privacidade, nomeadamente como ponto de partida para

([1]) 15 U.S.C. § 45(m); 16 C.F.R. § 1.98.

([2]) Ver *FTC, Business Center, Legal Resources*, https://www.ftc.gov/tips-advice/business-center/legal-resources?type=case&field-consumer-protection-topics-tid=251.

a partilha de informações a fim de assegurar uma proteção coordenada e mais eficaz aos consumidores. Aguardamos com expectativa a continuação do trabalho com as autoridades participantes da UE para o lançamento do sistema de alerta da GPEN mais amplamente e o desenvolvimento de outros instrumentos para melhorar a cooperação em matéria de execução nos casos relativos à proteção da privacidade, nomeadamente os que dizem respeito ao quadro.

A FTC tem o prazer de confirmar o seu compromisso de aplicar o novo quadro do Escudo de Proteção da Privacidade. Aguardamos igualmente com expectativa a continuação do envolvimento com os nossos colegas da UE, à medida que trabalhamos em conjunto para proteger a privacidade dos consumidores em ambos os lados do Atlântico.

Queira aceitar a expressão da minha mais elevada consideração,

Edith Ramirez

Presidente

Apêndice A

O Escudo de Proteção da Privacidade UE-EUA no seu contexto: uma panorâmica do sistema jurídico dos EUA em matéria de proteção da privacidade e da segurança

A proteção assegurada pelo quadro do Escudo de Proteção da Privacidade UE-EUA (a seguir denominado «quadro») existe no contexto das mais amplas proteções do respeito da privacidade garantidas pelo sistema jurídico dos Estados Unidos no seu conjunto. Em primeiro lugar, a *Federal Trade Commission* («FTC») dos EUA tem um programa sólido em matéria de proteção da privacidade e da segurança que abrange as práticas comerciais dos EUA e protege os consumidores do mundo inteiro. Em segundo lugar, o sistema jurídico dos Estados Unidos da proteção da privacidade e da segurança dos consumidores evoluiu consideravelmente desde 2000, ano em que foi adotado o programa inicial «porto seguro» EUA--UE. Desde então, foram promulgadas muitas leis federais e estaduais em matéria de privacidade e de segurança e o número de processos judiciais intentados por entidades públicas e privadas com vista ao exercício do direito à privacidade aumentou significativamente. As medidas de proteção previstas pelo sistema jurídico americano em matéria de proteção da privacidade e de segurança dos consumidores aplicáveis às práticas comerciais dos Estados Unidos completam, pelo seu amplo âmbito de aplicação, as medidas de proteção oferecidas aos cidadãos da UE ao abrigo do novo quadro.

I. PROGRAMA GERAL DA FTC PARA O CONTROLO DO RESPEITO DA PRIVACIDADE E DA SEGURANÇA

A FTC é a principal entidade de proteção dos consumidores nos EUA no que diz respeito à privacidade no setor comercial. Tem o poder de perseguir os atos e as práticas desleais ou enganosas que infringem a privacidade do consumidor e de fazer respeitar as leis destinadas sobretudo à proteção de determinadas informações financeiras e sanitárias, de informações sobre menores e as utilizadas para decidir da admissibilidade do consumidor a determinados benefícios.

A FTC tem uma experiência sem igual no respeito pela privacidade dos consumidores. As ações coercivas por ela adotadas diziam respeito a práticas ilícitas realizadas tanto em linha como fora de linha. Por exemplo, a FTC tomou medidas coercivas contra empresas muito conhecidas como Google, Facebook, Twitter, Microsoft, Wyndham, Oracle, HTC e Snapchat, assim como contra empresas menos conhecidas. Intentou ações judiciais contra empresas acusadas de ter inundado os consumidores de mensagens indesejadas (*spam*), de ter instalado *software* espião nos seus computadores, de não ter assegurado a proteção das informações pessoais dos consumidores, de rastrear os consumidores em linha de forma enganosa, de violar a privacidade de menores, de recolher indevidamente informações dos consumidores em dispositivos móveis e de não ter protegido adequadamente os dispositivos ligados à Internet utilizados para armazenar as informações pessoais. Em geral, as decisões tomadas na sequência de tais ações implicaram um controlo continuado por parte da FTC por um período de vinte anos, impediram novas infrações à lei e aplicaram às empresas sanções pecuniárias substanciais no caso de incumprimento da decisão ([1]). Deve observar-se que a decisão da FTC não protege apenas a pessoa que apresentou a queixa, mas sim todos os consumidores que se relacionarão no futuro com a empresa. A nível transfronteiras, a FTC tem competência para proteger os consumidores de todo o mundo das práticas realizadas nos Estados Unidos ([2]).

Até à data, a FTC deu início a mais de 130 casos de *spam* e de *software* espião, mais de 120 casos de infração à proibição de contacto telefónico no âmbito do telemarketing, mais de 100 ações no quadro da lei sobre a informação correta em matéria de crédito, quase 60 casos sobre a segurança dos dados, mais de 50 casos em matéria de proteção da privacidade em geral, mais de 30 casos de infração à lei Gramm-Leach-Bliley e mais de 20 ações coercivas ao abrigo da lei sobre a proteção da privacidade dos menores em linha (*Children's Online Privacy Protection Act* — «COPPA») ([3]). Para além destes casos, a FTC emanou e publicou cartas de aviso ([4]).

([1]) Qualquer entidade que não dê cumprimento a uma decisão da FTC é suscetível de sofrer uma sanção pecuniária num montante até 16 000 USD por cada infração, ou 16 000 USD por dia, em caso de infração continuada. *Ver* 15 U.S.C. § 45(l); 16 C.F.R. § 1.98(c).

([2]) O Congresso confirmou expressamente a competência da FTC para pedir junto dos tribunais medidas corretivas, incluindo a restituição, relativamente a atos ou práticas inerentes ao comércio internacional 1) que causam ou são suscetíveis de causar danos razoavelmente previsíveis nos Estados Unidos ou 2) que implicam uma conduta significativa nos Estados Unidos. *Ver* 15 U.S.C. § 45(a)(4).

([3]) Em alguns casos, os casos da FTC em matéria de privacidade e de segurança dos dados alegam que uma empresa adota práticas desleais e enganosas; estes casos também são por vezes caracterizados por alegadas violações de diversos instrumentos legislativos como a*Fair Credit Reporting Act*, a *Gramm-Leach-Bliley Act* e a COPPA.

([4]) Ver, por exemplo, *Press Release, Fed. Trade Comm'n, FTC Warns Children's App Maker BabyBus About Potential COPPA Violations* (22 de dezembro de 2014), https://www.ftc.gov/news-events/press-releases/2014/12/ftc-warns-childrens-app-maker-babybus-about-potential-coppa; *Press Release, Fed. Trade Comm'n, FTC Warns Data Broker Operations of Possible Privacy Violations* (7 de maio de 2013), https://www.ftc.gov/news-events/press-releases/2013/05/ftc-warns-data-broker-operations-possible-privacy-violations; *Press Release, Fed. Trade Comm'n, FTC Warns Data Brokers That Provide Tenant Rental Histories They May Be Subject to Fair Credit Reporting Act* (3 de abril de 2013), https://www.ftc.gov/news-events/press-releases/2013/04/ftc-warns-data-brokers-provide-tenant-rental-histories-they-may.

Em linha com esta tradição de aplicação rigorosa de medidas coercivas de proteção da privacidade, a FTC também examinou potenciais infrações do programa «porto seguro». Desde que este foi adotado, a FTC lançou de sua própria iniciativa investigações para verificar a conformidade ao «porto seguro» e deu início a 39 processos contra empresas dos EUA por violação deste programa. A FTC continuará a adotar esta abordagem proativa, considerando uma prioridade a aplicação coerciva do novo quadro.

II. MEDIDAS DE PROTEÇÃO DA PRIVACIDADE DOS CONSUMIDORES A NÍVEL FEDERAL E ESTADUAL

O resumo das modalidades e aplicação do «porto seguro», em anexo à decisão da Comissão Europeia sobre a adequação do programa «porto seguro», fornece uma síntese das numerosas leis federais e estaduais sobre a proteção da privacidade em vigor nos EUA em 2000, ano de adoção do programa «porto seguro» ([1]). Nessa altura, muitas leis federais regulavam a recolha e a utilização de informações pessoais no comércio, para além da secção 5 da *FTC Act*, designadamente: a *Cable Communications Policy Act*, a *Driver's Privacy Protection Act*, a *Electronic Communications Privacy Act*, a *Electronic Funds Transfer Act*, a *Fair Credit Reporting Act*, a *Gramm-Leach-Bliley Act*, a *Right to Financial Privacy Act*, a *Telephone Consumer Protection Act* e a *Video Privacy Protection Act*. Muitos Estados tinham legislação análoga nestes domínios.

Desde 2000, registou-se uma grande evolução tanto a nível federal como estadual que conferiram uma proteção adicional à privacidade dos consumidores ([2]). A nível federal, por exemplo, em 2013 a FTC alterou a norma relativa à COPPA, de modo a acrescentar uma proteção adicional às informações pessoais relativas a menores. A FTC emanou igualmente duas normas de execução da *Gramm- Leach-Bliley Act* (a lei sobre o respeito da privacidade — *Privacy Rule* — e a lei em matéria de garantias — *Safeguards Rule*), com base nas quais, as instituições financeiras ([3]) devem comunicar as práticas seguidas para a partilha das informações e dar execução a um programa geral de seguranças da informações destinado a proteger as informações relativas aos consumidores ([4]). Da mesma forma, a lei relativa à imparcialidade e à fiabilidade das operações de crédito (*Fair and Accurate Credit Transactions Act* — «FACTA»), adotada em 2003, completa as leis em matéria de crédito, em vigor desde longa data nos EUA, introduzindo obrigações relativas ao ocultação, partilha e eliminação de alguns dados financeiros sensíveis. A FTC emanou várias normas nos termos da FACTA relativas, nomeadamente, ao direito do consumidor de receber gratuitamente um relatório anual de solvabilidade; à obrigação de eliminação em condições seguras das informações sobre o consumidor; ao direito do consumidor de recusar receber determinadas ofertas de crédito ou de seguros; ao direito do consumidor de recusar a utilização de dados fornecidos por uma filial para comercializar os seus produtos e serviços; e à obrigação das instituições financeiras e dos credores de executar programas de deteção e de prevenção de usurpação de identidade ([5]). Além disso, os regulamentos adotados em execução da lei relativa à portabilidade e à responsabilização em matéria de seguro de saúde (*Health Insurance Portability and Accountability Act — HIPAA*) foram revistos em 2013, tendo sido introduzidas medidas de proteção adicionais para assegurar o respeito da privacidade e a segurança dos dados de saúde de caráter pessoal ([6]). Também entraram em vigor regras que protegem os consumidores de chamadas de telemarketing indesejadas, de chamadas automatizadas e de correios eletrónicos não desejados (*spam*). Por outro lado, o Congresso promulgou leis que exigem que certas empresas que recolhem dados de saúde assinalem eventuais infrações aos consumidores ([7]).

Os Estados também têm estado muito ativos na promulgação de leis relacionadas com a proteção da privacidade e com a segurança. Desde 2000, 47 Estados federados, mais o Distrito de Columbia, Guam, Porto Rico e as Ilhas Virgens promulgaram leis que impõem às empresas que informem os interessados em caso de violação da segurança das

([1]) Ver *U.S. Dep't of Commerce, Safe Harbor Enforcement Overview*, https://build.export.gov/main/safeharbor/eu/eg_main_018476.

([2]) Para uma síntese mais pormenorizada da proteção jurídica nos Estados Unidos, ver Daniel J. Solove & Paul Schwartz, *Information Privacy Law* (5.ª ed. 2015).

([3]) As instituições financeiras são definidas de forma muito geral na *Gramm-Leach-Bliley Act*, incluindo todas as empresas que «se consagram em larga medida» ao fornecimento de produtos e serviços financeiros. Esta definição inclui, por exemplo, as empresas de pagamento de cheques, as sociedades de empréstimo sobre salário, os corretores de hipotecas, as sociedades de empréstimo não bancários, os avaliadores do património pessoal ou imobiliário e os compiladores profissionais de declarações fiscais.

([4]) Nos termos da*Consumer Financial Protection Act* de 2010 («CFPA»), Título X da Pub. L. 111-203, 124 Stat. 1955 (21 de julho de 2010) (também conhecida como «*Dodd-Frank Wall Street Reform and Consumer Protection Act*»), a maior parte das competências de decisão da FTC ao abrigo da *Gramm-Leach-Bliley Act* foram transferidas para o *Consumer Financial Protection Bureau* («CFPB»). A FTC continua a ser a autoridade com poderes coercivos nos termos da *Gramm-Leach- Bliley ACT*, bem como a autoridade com competências de decisão em matéria de *Safeguards Rule*, conservando competências de decisão limitadas no âmbito da *Privacy Rule*, no que respeita aos concessionários de automóveis.

([5]) No âmbito da CFPA, a comissão partilha com o CFPB o seu papel de controlo da aplicação da FCRA, mas o essencial das competências de decisão são transferidas para o CFPB (com exceção da norma em matéria de usurpação de identidade — *Red Flags Rule* — e de eliminação de informações — *Disposal Rule*).

([6]) Ver 45 C.F.R. pts. 160, 162, 164.

([7]) Ver, por exemplo, *American Recovery & Reinvestment Act* de 2009, Pub. L. No. 111-5, 123 Stat. 115 (2009) e regulamentos pertinentes, 45 C.F.R. § § 164.404-164.414; 16 C.F.R. pt. 318.

informações pessoais ([1]). Em pelo menos 32 Estados mais Porto Rico estão em vigor leis sobre a eliminação dos dados, que impõem obrigações relativamente à destruição ou à eliminação das informações pessoais ([2]). Vários Estados adotaram igualmente leis sobre a segurança dos dados em geral. Além disso, a Califórnia adotou várias leis em matéria de proteção de privacidade, entre as quais uma que obriga as empresas a adotar políticas de proteção da privacidade e a divulgar as práticas seguidas quanto à não rastreabilidade ([3]), uma lei denominada «*Shine the Light*» que impõe maior transparência aos intermediários de dados ([4]) e uma lei que obriga a colocar à disposição um botão «apagar» que permite aos menores pedir a eliminação de algumas informações das redes sociais ([5]). Aplicando as referidas leis e exercendo outros poderes, o governo federal e os governos estaduais aplicaram sanções pecuniárias substanciais às empresas que não protegeram adequadamente a privacidade e a segurança das informações pessoais relativas aos consumidores ([6]).

Ações intentadas por particulares também conduziram a sentenças e transações favoráveis que preveem medidas de proteção adicionais em matéria de proteção da privacidade e de segurança dos dados dos consumidores. Por exemplo, em 2015, a empresa Target aceitou pagar 10 milhões de USD no âmbito de uma transação com clientes que alegavam que os seus dados pessoais de carácter financeiro tinham sido objeto de uma violação em grande escala. Em 2013, a AOL aceitou pagar, no quadro de uma transação, 5 milhões de USD para pôr fim a uma ação coletiva («*class action*») cujos autores alegavam uma anonimização insuficiente relacionada com a divulgação de pedidos de pesquisa de centenas de milhares de membros da AOL. Além disso, um tribunal federal homologaram um pagamento de 9 milhões de USD imposto à Netflix por ter conservado os históricos de locação em violação da lei sobre o respeito da privacidade no âmbito do fornecimento de material vídeo (*Video Privacy Protection Act*) de 1988. Na Califórnia, os tribunais federais homologaram duas transações diferentes com Facebook — uma no montante de 20 milhões de USD e outra no montante de 9,5 milhões de USD relativamente à recolha, utilização e partilha por esta empresa de dados pessoais dos seus utilizadores. Por último, em 2008, um tribunal do Estado da Califórnia homologou uma transação que impôs à empresa LensCrafters o pagamento de 20 milhões de USD pela divulgação ilícita de informações médicas dos consumidores.

No fim de contas, como o demonstra o presente resumo, os Estados Unidos asseguram aos consumidores uma proteção jurídica não negligenciável no domínio da proteção da privacidade e da segurança. O novo quadro do Escudo de Proteção da Privacidade, que proporciona aos cidadãos da União Europeia garantias significativas inscrever-se-á neste contexto mais amplo, em que a proteção da privacidade e da segurança dos consumidores continuará a ser uma prioridade importante.

([1]) Ver, por exemplo, *National Conference of State Legislatures* («NCSL»), *State Security Breach Notification Laws* (4 de janeiro de 2016), *disponível em* http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

([2]) NCSL, *Data Disposal Laws* (12 de janeiro de 2016), disponível em http://www.ncsl.org/research/telecommunications-and-information-technology/data-disposal-laws.aspx.

([3]) *Cal. Bus. & Professional Code* §§ 22575-22579.

([4]) *Cal. Civ. Code* §§ 1798.80-1798.84.

([5]) *Cal. Bus. & Professional Code* §§ 22580-22582.

([6]) Ver Jay Cline, *U.S. Takes the Gold in Doling Out Privacy Fines*, Computerworld (Feb. 17, 2014), disponível em: http://www.computerworld.com/s/article/9246393/Jay-Cline-U.S.-takes-the-gold-in-doling-out-privacy-fines?taxonomyId=17&pageNumber=1.

ANEXO V

Carta do Secretário dos Transportes dos EUA, Anthony Foxx

19 de fevereiro de 2016

Comissária Vera Jourová
Comissão Europeia
Rue de la Loi/Wetstraat 200
1049 l049 Bruxelas
Bélgica

Re: Escudo de Proteção da Privacidade UE-EUA

Excelentíssima Senhora Comissária Vera Jourová:

O *Department of Transportation* («DOT») dos Estados Unidos aprecia a oportunidade de descrever o seu papel na aplicação do Escudo de Proteção da Privacidade UE-EUA. O presente quadro desempenha um papel fundamental na proteção dos dados pessoais fornecidos durante transações comerciais num mundo cada vez mais interligado. Permite que as empresas realizem operações importantes na economia global, assegurando ao mesmo tempo que os consumidores da UE dispõem de proteções importantes em matéria de privacidade.

O DOT expressou publicamente pela primeira vez o seu compromisso de aplicar o quadro «porto seguro» numa carta enviada à Comissão Europeia há mais de 15 anos. O DOT comprometeu-se a aplicar decididamente os princípios da privacidade em «porto seguro» nessa carta. O DOT continua a manter o seu compromisso, que é recordado na presente carta.

Nomeadamente, o DOT renova o seu compromisso nos seguintes domínios fundamentais: 1) atribuição de prioridade à investigação de alegadas violações do Escudo de Proteção da Privacidade; 2) medidas de execução adequadas contra as entidades que façam alegações falsas ou enganosas relativamente à certificação de adesão ao Escudo de Proteção da Privacidade; e 3) acompanhamento e publicação de despachos de execução relativos a violações do Escudo de Privacidade. Apresentamos informações sobre cada um destes compromissos e, no que se refere ao contexto necessário, os antecedentes pertinentes sobre o papel do DOT na proteção da privacidade dos consumidores e na aplicação do quadro do Escudo de Proteção da Privacidade.

I. ANTECEDENTES

A. **Autoridade do DOT em matéria de proteção da privacidade**

O *Department of Transportation* encontra-se fortemente empenhado em assegurar a proteção da privacidade das informações fornecidas pelos consumidores às companhias aéreas e às agências de viagens. A autoridade do DOT para tomar medidas neste domínio encontra-se em 49 U.S.C. 41712, que proíbe uma transportadora aérea ou agência de viagens de adotar «práticas desleais ou enganosas e métodos desleais de concorrência» na venda de passagens aéreas, práticas essas que sejam ou possam ser prejudiciais para o consumidor. A secção 41712 segue o modelo da secção 5 da *Federal Trade Commission Act* (FTC) (15 U.S.C. 45). Interpretamos que a nossa legislação relativa às práticas desleais ou enganosas proíbe as companhias aéreas e as agências de viagens de: 1) infringir as disposições previstas na sua política em matéria de privacidade; ou 2) recolher ou divulgar informações privadas de uma forma que infrinja a ordem pública, seja imoral ou cause danos significativos aos consumidores não contrabalançados por benefícios compensatórios. Interpretamos igualmente que a secção 41712 proíbe as transportadoras e as agências de viagens de: 1) violar qualquer regra emitida pelo *Department of Transportation* que identifique práticas específicas relativas à privacidade como desleais ou enganosas; ou 2) infrinja a *Children's Online Privacy Protection Act* (COPPA) ou a regras da FTC que dão execução à COPPA. Nos termos da legislação federal, o DOT dispõe de competência exclusiva para regular as práticas de proteção da privacidade das companhias aéreas e partilha competência com a FTC no que se refere às práticas de proteção da privacidade das agências de viagens na venda de passagens aéreas.

Como tal, depois de uma transportadora ou um vendedor de passagens aéreas se comprometer publicamente a cumprir os princípios de privacidade do Escudo de Proteção da Privacidade, o *Department of Transportation* pode utilizar as competências jurídicas da secção 41712 para assegurar a observância desses princípios. Portanto, quando um passageiro fornece informações a uma transportadora ou a uma agência de viagens que se tenha comprometido a observar os princípios de privacidade do Escudo de Proteção da Privacidade, qualquer incumprimento por parte da transportadora ou da agência de viagens constituiria uma violação da secção 41712.

B. **Práticas de execução**

O *Office of Aviation Enforcement and Proceedings* (*Aviation Enforcement Office*) do *Department of Transportation* realiza investigações e instaura ações nos termos do título 49, secção 41712, do U.S.C. Dá execução à proibição legal constante da secção 41712 contra as práticas desleais e enganosas sobretudo através de negociação, da elaboração de decisões para cessar e proibir as referidas práticas, e da elaboração de despachos de avaliação de sanções civis. A referida entidade toma conhecimento de potenciais violações sobretudo a partir das queixas que recebe de cidadãos, agências de viagens, companhias aéreas e organismos governamentais norte-americanos e estrangeiros. Os consumidores podem utilizar o sítio Web do DOT para apresentar queixas relacionadas com a proteção da privacidade contra companhias aéreas e agências de viagens ([1]).

Caso não se chegue a um acordo razoável e adequado num determinado caso, o *Aviation Enforcement Office* tem competência para instituir um processo de execução que implica uma audição de provas perante um juiz de direito administrativo (JDA) do DOT. O JDA tem competência para emitir decisões para fazer cessar e proibir as práticas desleais, bem como sanções civis. Uma violação da secção 41712 pode resultar na emissão de uma decisão para fazer cessar e proibir as práticas denunciadas e na imposição de sanções de caráter civil até 27 500 USD por cada violação da secção 41712.

O *Department of Transportation* não tem competência para conceder indemnizações nem reparações pecuniárias aos queixosos. Todavia, o *Department of Transportation* tem autoridade para aprovar acordos resultantes de investigações instruídas pelo seu *Aviation Enforcement Office* que beneficiem diretamente os consumidores (por exemplo, dinheiro, vales) como compensação pelas sanções pecuniárias que, de outro modo, seriam pagas ao governo dos EUA. Já o fizemos e podemos fazê-lo no contexto dos princípios do quadro do Escudo de Proteção da Privacidade se as circunstâncias o justificarem. Uma violação repetida da secção 41712, por uma companhia aérea, também levantará questões relativas à disposição de cumprimento da companhia que pode, em situações extremas, levar a considerar que uma companhia aérea não tem condições para operar e, consequentemente, perder a sua licença de exploração.

Até à data, o DOT recebeu relativamente poucas queixas relativas a alegadas violações da privacidade por agências de viagens ou companhias aéreas. Sempre que surgem, são investigadas em conformidade com os princípios estabelecidos acima.

C. **Proteções jurídicas do DOT que beneficiam os consumidores da UE**

Nos termos da secção 41712, a proibição de práticas desleais ou enganosas no transporte aéreo ou na venda de passagens aéreas é aplicável às transportadoras, bem como às agências de viagens norte-americanas e estrangeiras. O DOT instaura frequentemente ações contra companhias aéreas norte-americanas e estrangeiras por práticas que afetam tanto os consumidores norte-americanos como estrangeiros com base no facto de que as práticas da companhia aérea se verificaram no âmbito da prestação de transporte de ou para os Estados Unidos. O DOT utiliza e continuará a utilizar todas as vias de recurso disponíveis para proteger os consumidores norte-americanos e estrangeiros de práticas desleais ou enganosas no transporte aéreo por entidades reguladas.

Além disso, o DOT aplica, no que diz respeito às companhias aéreas, outras leis seletivas cujas proteções são alargadas aos consumidores de países terceiros, tais como a COPPA. Entre outras coisas, a COPPA exige que os operadores de sítios Web e serviços em linha orientados para crianças, ou sítios destinados ao público em geral que reconhecidamente recolhem informações pessoais de crianças com idade inferior a 13 anos, apresentem um aviso aos pais e obtenham o consentimento verificável dos mesmos. Os serviços e sítio Web sediados nos EUA que são objeto da COPPA e recolhem informações pessoais de crianças estrangeiras são obrigados a respeitar a COPPA. Os serviços em linha e sítios Web sediados no estrangeiro também devem respeitar a COPPA se forem orientados para crianças nos Estados Unidos ou se recolherem reconhecidamente informações pessoais de crianças nos Estados Unidos. Se as companhias norte-americanas ou estrangeiras que exercem atividades nos Estados Unidos violarem a COPPA, o DOT teria competência para tomar medidas de execução.

II. APLICAÇÃO DO ESCUDO DE PROTEÇÃO DA PRIVACIDADE

Se uma companhia aérea ou uma agência de viagens optar por participar no quadro do Escudo de Proteção da Privacidade e o *Department of Transportation* receber uma queixa de que tal companhia aérea ou agência de viagens alegadamente violou o quadro, o *Department of Transportation* tomaria as medidas abaixo para aplicar decididamente o quadro.

([1]) http://www.transportation.gov/airconsumer/privacy-complaints.

A. **Atribuição de prioridade à investigação de alegadas violações**

O *Aviation Enforcement Office* do *Department of Transportation* investigará cada queixa que alegue violações do Escudo de Proteção da Privacidade (nomeadamente queixas recebidas de autoridades responsáveis pela proteção dos dados da UE) e tomará medidas de execução sempre que existam provas de uma violação. Além disso, o *Aviation Enforcement Office* cooperará com a FTC e o *Department of Commerce* e atribuirá prioridade à análise das alegações de que as entidades reguladas não respeitam os compromissos em matéria de proteção da privacidade assumidos no âmbito do quadro do Escudo de Proteção da Privacidade.

Após a receção de uma alegação de violação do Escudo de Proteção da Privacidade, o *Aviation Enforcement Office* do *Department of Transportation* pode tomar várias medidas no âmbito da sua investigação. Por exemplo, pode proceder à análise das políticas em matéria de proteção da privacidade da agência de viagens ou da companhia aérea, obter informações adicionais junto das mesmas ou de terceiros, proceder ao acompanhamento junto da entidade que submeteu a queixa e avaliar se existe um padrão de violações ou um número significativo de consumidores afetados. Além disso, determinaria se a questão implica assuntos no âmbito do *Department of Commerce* ou da FTC, avaliaria se a educação dos consumidores e das empresas seria útil e, conforme adequado, daria início a um processo de execução.

Caso o *Department of Transportation* tome conhecimento de possíveis violações do Escudo de Proteção da Privacidade por parte de agências de viagens, trabalhará em colaboração com a FTC nesta questão. Também informaremos a FTC e o *Department of Commerce* sobre o resultado das medidas de execução relativas ao Escudo de Proteção da Privacidade.

B. **Resolução de alegações falsas ou enganosas de participação**

O *Department of Transportation* continua a estar empenhado em investigar violações do Escudo de Proteção da Privacidade, nomeadamente alegações falsas ou enganosas de participação no programa do Escudo de Proteção da Privacidade. Atribuiremos prioridade à apreciação das queixas submetidas pelo *Department of Commerce* sobre organizações que identifique que aleguem indevidamente ser membros atuais do Escudo de Proteção da Privacidade ou que utilizem a respetiva marca de certificação sem autorização.

Além disso, salientamos que se a política em matéria de proteção da privacidade de uma empresa promete que cumpre os princípios significativos do Escudo de Proteção da Privacidade, a não efetuação ou manutenção de um registo junto do *Department of Commerce* provavelmente não irá, por si só, isentar a organização da execução desses compromissos por parte do DOT.

C. **Acompanhamento e publicação de despachos de execução relativos à infrações aos Escudo de Proteção da Privacidade**

O *Aviation Enforcement Office* do *Department of Transportation* também continua empenhado no acompanhamento dos despachos de execução, conforme necessário para assegurar a conformidade com o programa do Escudo de Proteção da Privacidade. Especificamente, se a referida entidade emitir uma decisão que cesse ou proíba futuras violações, por parte de uma companhia aérea ou agência de viagens, do Escudo de Proteção da Privacidade e da secção 41712, esta controlará a observância da disposição de cessação ou proibição constante da decisão. Além disso, a referida entidade assegurará que as decisões resultantes dos processos relativos ao Escudo de Proteção da Privacidade se encontram disponíveis no seu sítio Web.

Aguardamos com expectativa a continuação do trabalho com os nossos parceiros federais e partes interessadas da UE sobre questões relacionadas com o Escudo de Proteção da Privacidade.

Espero que estas informações tenham utilidade e estou ao inteiro dispor de Vossa Excelência para quaisquer dúvidas ou informações de que necessite.

Queira Vossa Excelência aceitar a expressão da minha mais elevada consideração,

Anthony R. Foxx

Secretário dos Transportes

ANEXO VI

Carta do Conselheiro-Geral Robert Litt

Office of the Director of National Intelligence (Gabinete do Diretor dos Serviços Nacionais de Informações)

22 de fevereiro de 2016

Justin S. Antonipillai
Conselheiro
Department of Commerce dos EUA
1401 Constitution Ave, NW
Washington, DC 20230

Ted Dean
Vice-Secretário Adjunto
International Trade Administration
1401 Constitution Ave, NW
Washington, DC 20230

Excelentíssimos Senhores Antonipillai e Dean:

Ao longo dos últimos dois anos e meio, no contexto das negociações para o Escudo de Proteção da Privacidade UE-EUA, os Estados Unidos forneceram informações significativas sobre o funcionamento da atividade de recolha de informação de origem eletromagnética por parte do setor das informações dos EUA. Tal incluiu informações sobre o quadro jurídico aplicável, a supervisão a vários níveis destas atividades, a elevada transparência sobre estas atividades e as proteções gerais da privacidade e das liberdades cívicas, a fim de assistir a Comissão Europeia no estabelecimento de uma decisão sobre a adequação dessas proteções no que diz respeito à derrogação por motivos de segurança nacional aos princípios do Escudo de Proteção da Privacidade. O presente documento resume as informações apresentadas.

I. PPD-28 E A REALIZAÇÃO DE ATIVIDADES DE INFORMAÇÃO DE ORIGEM ELETROMAGNÉTICA PELOS EUA

O setor das informações dos EUA recolhe informações externas de forma cuidadosa e controlada, em estrita conformidade com as leis dos EUA e sob reserva de múltiplos níveis de supervisão, incidindo sobre prioridades importantes em matéria de informação externa e segurança nacional. Um mosaico de leis e políticas regula a recolha de informação de origem eletromagnética dos EUA, nomeadamente a Constituição dos EUA, a *Foreign Intelligence Surveillance Act* (lei relativa à vigilância dos serviços de informações externas — 50 U.S.C. § 1801 *et seq.*) (FISA), o Decreto Executivo n.º 12333 e os respetivos procedimentos de execução, orientações presidenciais e inúmeros procedimentos e diretrizes, aprovados pelo Tribunal da FISA e o Procurador-Geral, que estabelecem regras adicionais que limitam a recolha, a preservação, a utilização e a divulgação de informações externas50 ([1]).

a. **Visão geral da PPD 28**

Em janeiro de 2014, o Presidente Obama proferiu um discurso que descreveu várias reformas às atividades de informação de origem eletromagnética e emitiu a *Presidential Policy Directive* 28 (PPD-28) relativa a estas atividades ([2]). O Presidente salientou que as atividades de informação de origem eletromagnética dos EUA ajudam a assegurar a proteção não apenas dos nosso país e das nossas liberdades, mas também a segurança e as liberdades de outros países, nomeadamente dos Estados-Membros da UE, que dependem das informações que os serviços de informações dos EUA obtêm para proteger os seus próprios cidadãos.

A PPD-28 estabelece uma série de princípios e requisitos aplicáveis a todas as atividades de informação de origem eletromagnética dos EUA e a todas as pessoas, independentemente da nacionalidade ou localização. Em especial, estabelece determinados requisitos aplicáveis aos procedimentos para lidar com a recolha, a preservação e a divulgação de informações pessoais sobre cidadãos de países terceiros adquiridas nos termos da informação de origem eletromagnética dos EUA. Estes requisitos são descritos em maior pormenor abaixo, mas em suma:

— A PPD reitera que os Estados Unidos recolhem informação de origem eletromagnética apenas da forma autorizada por lei, decreto executivo ou outra diretiva presidencial.

([1]) Encontram-se publicadas em linha e disponíveis ao público informações adicionais sobre as atividades de informações externas dos EUA através do setor das informações no *Record* (www.icontherecord.tumblr.com), o sítio Web público do ODNI dedicado à promoção de uma maior visibilidade pública no que diz respeito às atividades de informação do governo.

([2]) Disponível em https://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities.

— A PPD estabelece procedimentos com vista a assegurar que a atividade de recolha de informação de origem eletromagnética é realizada apenas para a consecução de objetivos de segurança nacional legítimos e autorizados.

— A PPD exige ainda que a privacidade e as liberdades cívicas constituam preocupações integrantes no planeamento das atividades de recolha de informação de origem eletromagnética. Nomeadamente, os Estados Unidos não recolhem informações com o objetivo de suprimir ou reprimir críticas ou dissidências; para prejudicar pessoas com base na sua etnia, raça, sexo, orientação sexual ou religião; ou para conferir uma vantagem comercial concorrencial às empresas e aos setores empresariais dos EUA.

— A PPD estabelece que a recolha de informação de origem eletromagnética deve ser a mais seletiva possível e que a informação de origem eletromagnética recolhida em larga escala só pode ser utilizada para efeitos específicos e enumerados.

— A PPD estipula que o setor das informações deve adotar procedimentos «razoavelmente concebidos para minimizar a divulgação e preservação de informações pessoais obtidas a partir de atividades de recolha de informação de origem eletromagnética,» e, nomeadamente, alargar determinadas proteções asseguradas às informações pessoais dos cidadãos norte-americanos às informações pessoais dos cidadãos de países terceiros.

— As normas de execução da PPD-28 dos organismos foram adotadas e publicadas.

A aplicabilidade dos procedimentos e proteções aqui estabelecidos ao Escudo de Proteção de Privacidade é clara. Sempre que tenham sido transferidos dados para empresas nos Estados Unidos nos termos do Escudo de Proteção da Privacidade, ou efetivamente por qualquer meio, os serviços de informações dos EUA podem solicitar esses dados às referidas empresas apenas se o pedido respeitar a FISA ou for efetuado nos termos de uma das disposições jurídicas da *National Security Letter* (carta de segurança nacional), que são discutidas abaixo ([1]). Além disso, sem confirmar nem desmentir as notícias veiculadas pelos meios de comunicação social que alegam que o setor das informações dos EUA recolhe informações de cabos transatlânticos enquanto estas são transmitidas para os Estados Unidos, se o setor das informações dos EUA recolhesse dados de cabos transatlânticos, procederia a tal sob reserva das limitações e garantias aqui estabelecidas, nomeadamente os requisitos da PPD-28.

b. **Limitações da recolha**

A PPD-28 estabelece vários princípios gerais importantes que regulam a recolha de informação de origem eletromagnética:

— A recolha de informação de origem eletromagnética deve ser permitida por lei ou por uma autorização presidencial e deve ser efetuada de acordo com a Constituição e a legislação.

— A privacidade e as liberdades cívicas devem ser considerações tomadas em conta no planeamento das atividades de recolha de informação de origem eletromagnética.

— A informação de origem eletromagnética será recolhida apenas quando existe um objetivo válido em matéria de informação ou contrainformação externa.

— Os Estados Unidos não recolherão informação de origem eletromagnética para suprimir ou reprimir críticas ou dissidências.

— Os Estados Unidos não recolherão informação de origem eletromagnética para prejudicar pessoas com base na sua etnia, raça, sexo, orientação sexual ou religião.

— Os Estados Unidos não recolherão informação de origem eletromagnética para conferir uma vantagem comercial concorrencial às empresas e aos setores empresariais dos EUA.

— A atividade de recolha de informação de origem eletromagnética deve ser *sempre* tão seletiva quanto possível, tomando em consideração a disponibilidade de outras fontes de informação. Tal significa que, entre outras coisas, sempre que possível, as atividades de recolha de informação de origem eletromagnética são realizadas de forma seletiva e não em larga escala.

O requisito de que a atividade de recolha informação de origem eletromagnética deve ser «tão seletiva quanto possível» é aplicável à forma de recolha da informação de origem eletromagnética, bem como ao que é efetivamente recolhido. Por exemplo, ao determinar se deve recolher informação de origem eletromagnética, o setor das informações deve tomar em

([1]) Os organismos regulamentares e responsáveis pela aplicação da lei podem solicitar informações às empresas para fins de investigação nos Estados Unidos nos termos de outras autoridades regulamentares, civis e penais que vão para além do âmbito do presente documento, que se limita às autoridades de segurança nacional.

consideração a disponibilidade de outras informações, incluindo fontes diplomáticas ou públicas, e atribuir prioridade à recolha através desses meios, sempre que adequado e viável. Além disso, as políticas dos elementos do setor das informações devem exigir que, sempre que possível, a recolha incida sobre alvos ou temas de informação externa específicos através da utilização de discriminantes (por exemplo, meios de comunicação específicos, termos de seleção e identificadores).

É importante analisar as informações fornecidas à Comissão como um todo. As decisões sobre o que é «viável» ou «possível» não são deixadas ao critério dos cidadãos, estando sujeitas às políticas que os organismos emitiram nos termos da PPD-28 — que foram disponibilizadas ao público — e aos restantes processos aí descritos ([1]). Tal como a PPD-28 estabelece, a recolha de informação de origem eletromagnética em larga escala é a recolha que «devido a considerações de caráter técnico ou operacional, é obtida sem a utilização de discriminantes (*por exemplo*, identificadores específicos, termos de seleção, etc.)». A este respeito, a PPD-28 reconhece que os elementos do setor das informações devem efetuar a recolha de informação de origem eletromagnética em larga escala em determinadas circunstâncias a fim de identificar ameaças novas ou emergentes, bem como outras informações de segurança nacional fundamentais que se encontram muitas vezes ocultadas no grande e complexo sistema das comunicações globais modernas. Reconhece ainda as preocupações relativas à privacidade e às liberdades cívicas suscitadas pela recolha de informação de origem eletromagnética em larga escala. Portanto, a PPD-28 estabelece que o setor das informações deve atribuir prioridade às alternativas que permitam a recolha seletiva de informação de origem eletromagnética ao invés da recolha de informação de origem eletromagnética em larga escala. Assim, sempre que possível, os elementos do setor das informações devem proceder a atividades de recolha seletiva de informação de origem eletromagnética em vez de atividades de recolha de informação de origem eletromagnética em larga escala ([2]). Estes princípios asseguram que a derrogação relativa à recolha em larga escala não se sobreporá à regra geral.

No que se refere ao conceito de «razoabilidade», este constitui um princípio de base do direito dos EUA. Significa que os elementos do setor das informações não serão obrigados a adotar qualquer medida teoricamente possível, mas terão de equilibrar os seus esforços de proteção dos interesses legítimos em matéria de privacidade e liberdades cívicas com as necessidades práticas das atividades de recolha informação de origem eletromagnética. Também aqui, as políticas dos organismos foram disponibilizadas e podem proporcionar garantias de que a expressão «razoavelmente concebidos para minimizar a divulgação e preservação de informações pessoais» não prejudica a regra geral.

A PPD-28 estabelece igualmente que a informação de origem eletromagnética recolhida em larga escala só pode ser utilizada para seis fins específicos: deteção e combate a determinadas atividades de potências estrangeiras; luta contra o terrorismo; luta contra a proliferação; cibersegurança; deteção e combate às ameaças para as forças armadas dos EUA ou dos aliados; e combate às ameaças criminosas transnacionais, nomeadamente evasões a sanções. O *National Security Advisor* (conselheiro para a segurança nacional) do Presidente, em consulta com o diretor dos serviços nacionais de informações (DNI), reapreciará anualmente estas utilizações admissíveis da informação de origem eletromagnética recolhida em larga escala a fim de determinar se devem ser alteradas. O DNI disponibilizará, tanto quanto possível, esta lista ao público em conformidade com a segurança nacional. Isto constitui uma limitação importante e transparente à utilização da recolha de informação de origem eletromagnética em larga escala.

Além disso, os elementos do setor das informações que aplicam a PPD-28 reforçaram as normas e práticas analíticas existentes relativas à consulta de informação de origem eletromagnética não avaliada ([3]). Os analistas devem estruturar as suas questões ou outros termos de pesquisa e técnicas a fim de garantir que são adequados para identificar informações relevantes para uma missão de informação externa ou aplicação da lei válida. Para tal, os elementos do setor das informações devem centrar as questões sobre pessoas nas categorias de informação de origem eletromagnética que dão resposta a um requisito em matéria de informação externa ou aplicação da lei, a fim de evitar a utilização de informações pessoais não pertinentes para os requisitos de informação externa ou aplicação da lei.

É importante salientar que quaisquer atividades de recolha em larga escala no que se refere às comunicações na Internet que o setor das informações dos EUA realize através de informação de origem eletromagnética são efetuadas numa pequena proporção da Internet. Além disso, a utilização de consultas orientadas, tal como descrito acima, assegura que apenas os elementos que se considera deterem um potencial valor informativo são apresentados aos analistas para efeitos de análise. Estes limites visam proteger a privacidade e as liberdades cívicas de todas as pessoas, independentemente da sua nacionalidade e do seu local de residência.

([1]) Disponível em www.icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties#ppd-28. Estes procedimentos implementam os conceitos de orientação e seletividade debatidos na presente carta especificamente para cada elemento do setor das informações.

([2]) Para citar apenas um exemplo, os procedimentos da NSA que dão execução à PPD-28 afirmam que «[s]empre que possível, a recolha ocorrerá através da utilização de um ou mais termos de seleção a fim de centrar a recolha em alvos de informação externa específicos (*por exemplo*, um terrorista ou grupo de terroristas específico e conhecido) ou temas de informação externa específicos (*por exemplo*, a proliferação de armas de destruição maciça por uma potência estrangeira ou os seus agentes)».

([3]) Disponível em http://www.dni.gov/files/documents/1017/PPD-28_Status_Report_Oct_2014.pdf.

Os Estados Unidos dispõem de processos exaustivos para garantir que as atividades de recolha de informação de origem eletromagnética são realizadas apenas para a consecução de objetivos de segurança nacional adequados. Anualmente, o Presidente estabelece as prioridades mais elevadas do país no que se refere à recolha de informações externas após um processo interinstitucional formal. alargado. O DNI é responsável pela tradução destas prioridades em matéria de informação no *National Intelligence Priorities Framework* (quadro das prioridades dos serviços de informações nacionais) ou NIPF. A PPD-28 reforçou e melhorou o processo interinstitucional a fim de assegurar que todas as prioridades de informação do setor das informações são revistas e aprovadas por decisores políticos de alto nível. A *Intelligence Community Directive* (ICD) 204 apresenta orientações adicionais sobre o NIPF e foi atualizada em janeiro de 2015 a fim de integrar os requisitos da PPD-28 ([1]). Embora o NIPF seja classificado, as informações relacionadas com prioridades específicas dos EUA em matéria de informação externa são refletidas anualmente na *Worldwide Threat Assessment* do DNI que não é classificada e também se encontra disponível no sítio Web do ODNI.

As prioridades constantes do NIPF são de um nível de generalidade consideravelmente elevado. Incluem temas como a procura de capacidades em termos nucleares e de mísseis balísticos por parte de adversários estrangeiros específicos, os efeitos da corrupção dos cartéis de drogas e os abusos dos direitos humanos em países específicos. São aplicáveis não apenas à informação de origem eletromagnética, mas também a todas as atividades de recolha de informação. A organização responsável pela tradução das prioridades constantes do NIPF na recolha efetiva de informação de origem eletromagnética é denominada *National Signals Intelligence Committee* (comissão nacional de informação de origem eletromagnética), ou SIGCOM. Funciona sob a tutela do diretor da National Security Agency (Agência Nacional de Segurança — NSA), que é nomeado pelo Decreto Executivo n.º 12333 na qualidade de «administrador funcional da informação de origem eletromagnética,» responsável pela supervisão e coordenação da informação de origem eletromagnética em todo o setor das informações sob a supervisão do Secretário da Defesa e do DNI. A SIGCOM tem representantes de todos os elementos do setor das informações e, à medida que os Estados Unidos aplicam na íntegra a PPD-28, também contará com a plena representação de outros departamentos e organismos com um interesse político na informação de origem eletromagnética.

Todos os departamentos e organismos dos EUA que são consumidores de informação externa apresentam os seus pedidos de recolha à SIGCOM. A SIGCOM analisa esses pedidos, certifica-se de que são coerentes com o NIPF e atribui-lhes prioridades através dos seguintes critérios:

— Pode a informação de origem eletromagnética fornecer informações úteis neste caso ou será que existem fontes de informação melhores e mais eficazes em termos de custos para preencher o requisito, tais como imagens ou informação proveniente de fontes abertas?

— Quão crucial é esta necessidade de informação? Caso se trate de uma prioridade elevada no NIPF, muitas vezes será uma prioridade elevada em termos de informação de origem eletromagnética.

— Que tipo de informação de origem eletromagnética poderia ser utilizado?

— A recolha é a mais seletiva possível? Devem definir-se limites temporais, geográficos ou de outro tipo?

O processo relativo aos requisitos da informação de origem eletromagnética dos EUA também exige que sejam expressamente tomados em consideração outros fatores, a saber:

— É o alvo da recolha, ou a metodologia utilizada para a recolha, particularmente sensível? Caso tal se verifique, será necessária a reapreciação por decisores políticos de alto nível.

— Representará a recolha um risco indevido para a privacidade e as liberdades cívicas, independentemente da nacionalidade?

— São necessárias garantias adicionais em matéria de divulgação e preservação a fim de proteger interesses no domínio da segurança nacional ou da privacidade?

Por último, no final do processo, pessoal da NSA com formação adequada receberá as prioridades validadas pela SIGCOM e investigará e identificará termos de seleção específicos, tais como números de telefone ou endereços de correio eletrónico, que se espera que recolham informação externa que dê resposta a estas prioridades. Todos os seletores devem ser revistos e aprovados antes da sua introdução nos sistemas de recolha da NSA. Contudo, mesmo

([1]) Disponível em: http://www.dni.gov/files/documents/ICD/ICD%20204%20National%20Intelligence%20Priorities%20Framework.pdf.

nesses casos, se e quando a recolha ocorre efetivamente dependerá em parte de considerações adicionais, como a disponibilidade de recursos de recolha adequados. Este processo assegura que os alvos da recolha de informação de origem eletromagnética dos EUA refletem necessidades de informação externa válidas e importantes. E, como é evidente, sempre que a recolha seja realizada nos termos da FISA, a NSA e outros organismos devem seguir restrições adicionais aprovadas pelo *Foreign Intelligence Surveillance Court* (tribunal encarregado de supervisionar os pedidos e mandatos em matéria de vigilância). Em suma, nem a NSA nem qualquer outro serviço de informações dos EUA decide, por si só, o que recolher.

Em geral, este processo assegura que todas as prioridades dos EUA em termos de informação são estabelecidas por decisores políticos de alto nível que se encontram na melhor posição para identificar as necessidades do EUA em matéria de informação externa, e que esses decisores políticos tomam em consideração não apenas o potencial valor da recolha de informação, mas também os riscos associados a essa recolha, nomeadamente os riscos relacionados com a privacidade, interesses económicos nacionais e relações externas.

No respeitante aos dados transmitidos para os EUA ao abrigo do Escudo de Proteção da Privacidade, embora os Estados Unidos não possam confirmar nem desmentir operações ou métodos de recolha de informação específicos, os requisitos da PPD-28 são aplicáveis a todas as operações de recolha de informação de origem eletromagnética realizadas pelos Estados Unidos, independentemente do tipo ou da fonte dos dados recolhidos. Além disso, as limitações e garantias aplicáveis à recolha de informação de origem eletromagnética são aplicáveis à informação de origem eletromagnética recolhida para qualquer efeito autorizado, nomeadamente para efeitos de relações externas e segurança nacional.

Os procedimentos debatidos acima demonstram um compromisso evidente para evitar a recolha arbitrária e indiscriminada de informação de origem eletromagnética e aplicar — a partir dos níveis mais elevados do nosso governo — o princípio da razoabilidade. A PPD-28 e os procedimentos de execução dos organismos esclarecem as limitações novas e existentes e descrevem em maior pormenor a finalidade para a qual os Estados Unidos recolhem e utilizam a informação de origem eletromagnética. Estes devem garantir que as atividades de recolha de informação de origem eletromagnética são e continuarão a ser realizadas apenas para a consecução de objetivos legítimos em termos de informação externa.

c. **Limitações à preservação e divulgação**

A secção 4 da PPD-28 exige que cada elemento do setor das informações tenha limites expressos no que se refere à preservação e divulgação de informações pessoais sobre cidadãos de países terceiros recolhidas através de informação de origem eletromagnética, comparáveis aos limites estabelecidos para os cidadãos dos EUA. Estas regras são integradas nos procedimentos de cada organismo do setor das informações que foram divulgados em fevereiro de 2015 e estão disponíveis ao público. Para serem elegíveis para efeitos de preservação ou divulgação na qualidade de informações externas, as informações pessoais devem ser relativas a uma necessidade de informação autorizada, tal como determinado no processo do NIPF descrito acima; devem ser razoavelmente consideradas provas de um crime; ou devem cumprir uma das normas para a preservação de informações pessoais dos EUA identificadas no Decreto Executivo n.º 12333, secção 2.3.

As informações relativamente às quais não foi efetuada uma determinação não podem ser preservadas durante um período superior a cinco anos, a menos que o DNI determine expressamente que a preservação continuada faz parte dos interesses de segurança nacional dos EUA. Assim, os elementos do setor das informações devem eliminar as informações de cidadãos de países terceiros obtidas através da recolha de informação de origem eletromagnética cinco anos após a recolha, salvo se, por exemplo, se tenha determinado que as informações são relevantes para um requisito de informação externa autorizado, ou se o DNI determinar, depois de tomar em consideração o parecer do *Civil Liberties Protection Officer* (agente responsável pela proteção das liberdades cívicas) do ODNI e dos funcionários responsáveis pela proteção da privacidade e das liberdades cívicas, que a preservação continuada é do interesse da segurança nacional.

Além disso, todas as políticas dos organismos que dão execução à PPD-28 exigem agora expressamente que as informações sobre uma pessoa não sejam divulgadas simplesmente porque esta é cidadã de um país terceiro, e o ODNI emitiu uma diretiva a todos os elementos do setor das informações ([1]) para refletir este requisito. O pessoal do setor das informações é especificamente obrigado a tomar em consideração os interesses em matéria de privacidade dos cidadãos de países terceiros na elaboração e divulgação de relatórios sobre informações. Em especial, a informação de origem eletromagnética sobre as atividades quotidianas de um estrangeiro não seria considerada informação externa passível de divulgação ou preservação permanente por força simplesmente desse facto, a menos que dê resposta de outro modo a um requisito autorizado em matéria de informação externa. O que precede reconhece uma limitação importante e dá resposta às preocupações da Comissão Europeia sobre a amplitude da definição de informação externa estabelecida no Decreto Executivo 12333.

([1]) Intelligence Community Directive (ICD) 203, disponível em http://www.dni.gov/files/documents/ICD/ICD%20203%20Analytic%20Standards.pdf.

d. **Conformidade e supervisão**

O sistema norte-americano de supervisão da informação externa proporciona uma supervisão rigorosa e a vários níveis com o objetivo de assegurar a conformidade com as leis e os procedimentos aplicáveis, designadamente os relativos à recolha, preservação e divulgação de informações respeitantes a cidadãos de países terceiros obtidas através da recolha de informação de origem eletromagnética, tal como estipulado pela PPD-28. O que precede inclui o seguinte:

— O setor das informações emprega centenas de funcionários responsáveis pela supervisão. A NSA, por si só, dispõe de mais de 300 pessoas dedicadas à conformidade e outros elementos também dispõem de gabinetes de supervisão. Além disso, o *Department of Justice* procede à ampla supervisão das atividades de informação e o *Department of Defense* também efetua supervisão.

— Cada elemento do setor das informações dispõe do seu próprio *Office of the Inspector General* (Gabinete do Inspetor-Geral) com responsabilidade pela supervisão das atividades de informações externas, entre outras questões. Os Inspetores Gerais são juridicamente independentes; dispõem de amplas competências para realizar investigações, auditorias e reapreciações de programas, nomeadamente no que se refere a fraude e abuso ou violação da lei; e podem recomendar medidas corretivas. Embora as recomendações do inspetor-geral não sejam vinculativas, os relatórios do inspetor-geral são frequentemente disponibilizados ao público e, de qualquer forma, são apresentados ao Congresso; tal inclui relatórios de acompanhamento se as medidas corretivas recomendadas em relatórios anteriores ainda não tiverem sido concluídas. Portanto, o Congresso é informado de qualquer incumprimento e pode exercer pressão, designadamente através de meios orçamentais, a fim de aplicar medidas corretivas. Vários relatórios dos inspetores-gerais sobre programas de informações foram divulgados publicamente ([1]).

— O Civil Liberties and Privacy Office (gabinete responsável pela proteção da privacidade e das liberdades cívicas — CLPO) do ODNI é responsável por garantir que o setor das informações opera de modo a aumentar a segurança nacional, protegendo ao mesmo tempo as liberdades cívicas e os direitos relativos à proteção da privacidade. ([2]) Outros elementos do setor das informações dispõem dos seus próprios agentes responsáveis pela proteção da privacidade.

— A *Privacy and Civil Liberties Oversight Board* (comissão de controlo da privacidade e das liberdades cívicas — PCLOB), um organismo independente estabelecido por lei, é responsável por analisar e reapreciar programas e políticas de luta contra o terrorismo, nomeadamente a utilização de informação de origem eletromagnética, para garantir que protegem a privacidade e as liberdades cívicas de modo adequado. Emitiu vários relatórios públicos sobre as atividades de informação.

— Tal como discutido em pormenor adiante, o *Foreign Intelligence Surveillance Court*, um tribunal constituído por juízes federais independentes, é responsável pela supervisão e o cumprimento de quaisquer atividades de recolha de informação de origem eletromagnética realizadas nos termos da FISA.

— Por último, o Congresso dos EUA, especificamente as *House and Senate Intelligence and Judiciary Committees*, têm responsabilidades significativas de supervisão no que se refere a todas as atividades de informações externas dos EUA, designadamente a informação de origem eletromagnética.

Para além destes mecanismos de supervisão formal, o setor das informações dispõe de inúmeros mecanismos em vigor para garantir que o setor das informações cumpre as limitações aplicáveis à recolha descritas abaixo. Por exemplo:

— Os funcionários do Conselho são obrigados a validar os seus requisitos de informação de origem eletromagnética todos os anos.

— A NSA verifica os alvos de informação de origem eletromagnética durante todo o processo de recolha a fim de determinar se fornecem efetivamente informações externas valiosas que dão resposta às prioridades e cessará a recolha relativa a alvos em que tal não se verifique. Procedimentos adicionais asseguram que os termos de seleção são reapreciados periodicamente.

([1]) Ver, por exemplo, o relatório do Inspetor Geral do *Department of Justice* dos EUA «*A Review of the Federal Bureau of Investigation's Activities Under Section 702 of the Foreign Intelligence Surveillance Act of 2008*» (setembro de 2012), *disponível em* https://oig.justice.gov/reports/2016/o1601a.pdf.

([2]) Ver www.dni.gov/clpo.

— Com base numa recomendação de um grupo de revisão independente nomeado pelo Presidente Obama, o DNI instituiu um novo mecanismo para controlar a recolha e a divulgação de informação de origem eletromagnética especialmente sensível devido à natureza do alvo ou do meio de recolha, a fim de assegurar que são coerentes com as determinações dos decisores políticos.

— Por último, o ODNI revê anualmente a afetação de recursos do setor das informações em relação às prioridades do NIPF e à missão de informação como um todo. Esta revisão inclui avaliações do valor de todos os tipos de recolha de informações, nomeadamente informação de origem eletromagnética, e analisa o passado — quão bem-sucedido foi o setor das informações na consecução dos seus objetivos? — e o futuro — de que necessitará o setor das informações no futuro? Isto garante que os recursos da informação de origem eletromagnética são aplicados às prioridades nacionais mais importantes.

Tal como salientado pela presente visão geral abrangente, o setor das informações não decide de forma autónoma as conversas a que escuta, não tenta recolher tudo, nem opera sem qualquer escrutínio. As suas atividades incidem sobre as prioridades estabelecidas pelos decisores políticos, através de um processo que envolve o contributo de todo o governo e que é supervisionado pela NSA e o ODNI, o *Department of Justice* e o *Department of Defense*.

A PPD-28 também contém inúmeras outras disposições para garantir que as informações pessoais recolhidas nos termos da informação de origem eletromagnética são protegidas, independentemente da nacionalidade. Por exemplo, a PPD-28 prevê procedimentos de segurança, acesso e qualidade dos dados a fim de proteger as informações pessoais obtidas através da recolha de informação de origem eletromagnética e prevê formação obrigatória com o objetivo garantir que o pessoal compreende a responsabilidade de proteger as informações pessoais, independentemente da nacionalidade. A PPD prevê igualmente mecanismos de supervisão e conformidade adicionais. Estes incluem auditorias e reapreciações periódicas por funcionários adequados responsáveis pela supervisão e o cumprimento das práticas de proteção das informações pessoais constantes da informação de origem eletromagnética. As reapreciações devem examinar igualmente o respeito das agências pelos procedimentos de proteção de tais informações.

Além disso, a PPD-28 prevê que as situações graves de incumprimento relacionadas com cidadãos de países terceiros serão resolvidas a nível do quadro superior do governo. Caso se verifique uma situação grave de incumprimento relacionada com as informações pessoais de qualquer pessoa obtidas em consequência de atividades de recolha de informação de origem eletromagnética, a questão deve, para além de quaisquer requisitos de comunicação em vigor, ser imediatamente comunicada ao DNI. Se a questão for relativa às informações pessoais de um cidadão de um país terceiro, o DNI, em consulta com o Secretário de Estado e o chefe do elemento do setor de informações relevante, determinará se devem ser tomadas medidas para notificar o governo estrangeiro relevante, em consonância com a proteção das fontes, dos métodos e dos funcionários dos EUA. Além disso, tal como estabelecido pela PPD-28, o Secretário de Estado identificou uma alta funcionária, a Subsecretária Catherine Novelli, para exercer a função de ponto de contacto para os governos estrangeiros que desejem expressar preocupações sobre as atividades de recolha de informação de origem eletromagnética dos Estados Unidos. Este compromisso de envolvimento a alto nível exemplifica os esforços envidados pelo governo dos EUA nos últimos anos para inspirar confiança nas inúmeras e sobrepostas proteções da privacidade em vigor para as informações dos cidadãos dos EUA e de países terceiros.

e. **Resumo**

Os processos dos Estados Unidos para a recolha, preservação e divulgação de informações externas asseguram proteções da privacidade importantes para as informações pessoais de todas as pessoas, independentemente da nacionalidade. Nomeadamente, estes processos garantem que o nosso setor das informações se concentra na sua missão de segurança nacional, conforme autorizada pelas leis, os decretos executivos e as diretivas presidenciais aplicáveis; salvaguarda as informações do acesso, da utilização e da divulgação não autorizados; e realiza as suas atividades sob vários níveis de reapreciação e supervisão, nomeadamente por comissões de supervisão do Congresso. A PPD-28 e os respetivos procedimentos de execução representam os nossos esforços para alargar determinados princípios de minimização e outros princípios importantes em matéria de proteção dos dados às informações pessoais de todas as pessoas, independentemente da nacionalidade. As informações pessoais obtidas através da recolha de informação de origem eletromagnética por parte dos EUA estão sujeitas aos princípios e requisitos da legislação dos EUA e das orientações do Presidente, nomeadamente às proteções estabelecidas na PPD-28. Estes princípios e requisitos asseguram que todas as pessoas são tratadas com dignidade e respeito, independentemente da sua nacionalidade ou de onde possam residir, e reconhecem que todas as pessoas têm interesses de privacidade legítimos no tratamento das suas informações pessoais.

II. FOREIGN INTELLIGENCE SURVEILLANCE ACT — SECÇÃO 702

A recolha nos termos da secção 702 da *Foreign Intelligence Surveillance Act* ([1]) não é «maciça nem indiscriminada», incidindo estreitamente sobre a recolha de informações externas de alvos legítimos e individualmente identificados; é claramente autorizada por uma competência jurídica explícita; e é objeto de supervisão judicial independente, bem como de revisão e supervisão significativas no poder executivo e no Congresso. A recolha nos termos da secção 702 é considerada informação de origem eletromagnética sujeita aos requisitos da PPD-28 ([2]).

A recolha de acordo com a secção 702 constitui uma das mais valiosas fontes de informação que protegem tanto os Estados Unidos como os nossos parceiros europeus. Encontram-se disponíveis ao público informações abrangentes sobre a aplicação e a supervisão da secção 702. Inúmeros arquivos judiciais, decisões judiciais e relatórios de supervisão relacionados com o programa foram desclassificados e divulgados no sítio Web de divulgação pública do ODNI, www.icontherecord.tumblr.com. Além disso, a secção 702 foi amplamente analisada pela PCLOB, num relatório que se encontra disponível em https://www.pclob.gov/library/702-Report.pdf ([3]).

A secção 702 foi aprovada como parte da *FISA Amendments Act* de 2008, ([4]) após um amplo debate público no Congresso. Autoriza a obtenção de informações externas ao visar cidadãos de países terceiros localizados fora dos EUA, com a assistência obrigatória dos fornecedores de serviços de comunicações eletrónicas dos EUA. A secção 702 autoriza o Procurador-Geral e o DNI — dois funcionários a nível do Conselho nomeados pelo Presidente e confirmados pelo Senado — a apresentarem certificações anuais ao Tribunal da FISA ([5]). Estas certificações identificam categorias específicas de informações externas a recolher, tais como informações relacionadas com a luta contra o terrorismo ou armas de destruição maciça, que devem ser inseridas nas categorias de informações externas definidas pela FISA ([6]). Tal como a PCLOB salienta, «[e]stas limitações *não* permitem a recolha ilimitada de informações sobre estrangeiros» ([7]).

As certificações também devem incluir procedimentos de «orientação» e «minimização» que devem ser revistos e aprovados pelo Tribunal da FISA ([8]). Os procedimentos de orientação visam assegurar que a recolha é efetuada apenas de acordo com o que é autorizado por lei e que é abrangida pelo âmbito das certificações; os procedimentos de minimização visam limitar a obtenção, divulgação e preservação de informações sobre cidadãos dos EUA, mas contêm igualmente disposições que asseguram a proteção significativa das informações sobre cidadãos de países terceiros, descritas abaixo. Além disso, tal como descrito acima, na PPD-28, o Presidente estabeleceu que o setor das informações deve assegurar proteções adicionais para as informações pessoais relativas a cidadãos de países terceiros e tais proteções são aplicáveis às informações recolhidas nos termos da secção 702.

Quando o tribunal aprova os procedimentos de orientação e minimização, a recolha nos termos da secção 702 não é maciça nem indiscriminada, «consistindo na íntegra na incidência sobre pessoas específicas sobre as quais foi realizada uma determinação individualizada», tal como declarado pela PCLOB ([9]). A recolha é orientada através da utilização de seletores individuais, tais como endereços de correio eletrónico ou números de telefone, que o pessoal dos serviços de

([1]) 50 U.S.C. § 1881a.

([2]) Os Estados Unidos também podem obter ordens judiciais nos termos de outras disposições da FISA para a produção de dados, nomeadamente dados transferidos ao abrigo do Escudo de Proteção da Privacidade. *Ver* 50 U.S.C. § 1801 *et seq*. Títulos I e III da FISA, que, respetivamente, autorizam a vigilância eletrónica e buscas físicas, exigem uma decisão judicial (exceto em casos urgentes) e exigem sempre uma causa provável para considerar que o alvo é uma potência estrangeira ou um agente de uma potência estrangeira. O título IV da FISA autoriza a utilização de dispositivos de registo de chamadas telefónicas e comunicações eletrónicas, nos termos de uma decisão judicial (exceto em casos urgentes) em informação externa, contrainformação, ou investigações de luta contra o terrorismo autorizadas. O título V da FISA permite que o FBI, nos termos de uma decisão judicial (exceto em casos urgentes) obtenha documentação empresarial relevante para efeitos de informação externa, contrainformação, ou investigações de luta contra o terrorismo autorizadas. Tal como debatido abaixo, a *Freedom Act* proíbe especificamente a utilização de decisões relativas a dispositivos de registo de chamadas telefónicas e comunicações eletrónicas ou a documentação empresarial para a recolha em larga escala e estabelece um requisito de um «termo de seleção específico» a fim de garantir que as autoridades são utilizadas de modo orientado.

([3]) *Privacy and Civil Liberties Board*, «*Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*» (2 de junho de 2014) («relatório da PCLOB»).

([4]) Ver Pub. L. N.º 110-261, 122 Stat. 2436 (2008).

([5]) Ver 50 U.S.C. § 1881a(a) e (b).

([6]) Ver *id*. § 1801(e).

([7]) Ver relatório da PCLOB, p. 99.

([8]) Ver 50 U.S.C. § 1881a(d) e (e).

([9]) Ver Relatório da PCLOB, ponto 111.

informações dos EUA determinou serem provavelmente utilizados para comunicar informações externas do tipo englobado pela certificação apresentada ao tribunal ([1]). A fundamentação para a seleção do alvo deve ser documentada e a documentação relativa a cada seletor é subsequentemente revista pelo *Department of Justice* ([2]). O governo dos EUA divulgou informações que demonstram que, em 2014, cerca de 90 000 pessoas foram alvo de recolha de informações nos termos da secção 702, uma fração minúscula dos mais de três mil milhões de utilizadores da Internet em todo o mundo ([3]).

As informações recolhidas nos termos da secção 702 são objeto de procedimentos de minimização judicialmente aprovados, que asseguram proteções a cidadãos dos EUA e de países terceiros e que foram publicamente divulgados ([4]). Por exemplo, as comunicações obtidas ao abrigo da secção 702, quer sejam de cidadãos dos EUA ou de países terceiros, são armazenadas em base de dados com controlos de acesso rigorosos. Só podem ser revistas por pessoal dos serviços de informações com formação em procedimentos de minimização com vista à proteção da privacidade e cujo acesso tenha sido especificamente aprovado para o exercício das suas funções autorizadas ([5]). A utilização dos dados está limitada à identificação de informações externas ou provas de um crime ([6]). Nos termos da PPD-28, estas informações podem ser divulgadas apenas se existir um objetivo válido em matéria de aplicação da lei ou informação externa; o simples facto de uma parte na comunicação não ser um cidadão dos EUA não é suficiente ([7]). Além disso, os procedimentos de minimização e a PPD-28 também estabelecem limites relativos ao período durante o qual os dados obtidos nos termos da secção 702 podem ser preservados ([8]).

A supervisão da secção 702 é abrangente e é realizada pelos três poderes do nosso governo. As agências que dão execução à lei dispõem de vários níveis de reexame interno, nomeadamente por inspetores-gerais independentes, e controlos tecnológicos no que diz respeito ao acesso aos dados. O *Department of Justice* e o ODNI procedem à reapreciação e ao escrutínio pormenorizado da utilização da secção 702 para verificar a conformidade com as normas jurídicas; os organismos estão igualmente vinculados por uma obrigação independente de comunicar potenciais situações de incumprimento. Estas situações são investigadas e todas as situações de incumprimento são comunicadas ao *Foreign Intelligence Surveillance Court*, à *Intelligence Oversight Board* (comissão de supervisão dos serviços de informações) do Presidente e ao Congresso e são corrigidas de modo adequado. ([9]) Até à data, não se verificaram situações de tentativas voluntárias de violar a lei ou evadir requisitos jurídicos ([10]).

O Tribunal da FISA desempenha um papel importante na aplicação da secção 702. É constituído por juízes federais independentes que exercem funções durante um mandato de sete anos no Tribunal da FISA, mas que, como todos os juízes federais, dispõem de um posto vitalício como juízes. Tal como salientado acima, o Tribunal deve reapreciar as certificações anuais, bem como os procedimentos de orientação e minimização para determinar se são conformes com a legislação. Além disso, tal como igualmente sublinhado acima, o governo é obrigado a notificar imediatamente as situações de incumprimento ao Tribunal ([11]), e vários pareceres do Tribunal foram desclassificados e divulgados, demonstrando o nível extraordinário de independência e controlo judicial que exerce na apreciação dessas situações.

Os processos minuciosos do Tribunal foram descritos pelo seu antigo juiz presidente numa carta ao Congresso que foi publicamente divulgada ([12]). Além disso, em consequência da *Freedom Act*, descrita abaixo, o Tribunal está agora expressamente autorizado a nomear um advogado externo como representante independente da privacidade em processos que apresentem questões jurídicas novas ou significativas ([13]). Este grau de envolvimento do poder judiciário independente de um país nas atividades de informações externas que visam pessoas que não são cidadãs desse país nem se encontram no mesmo é pouco comum e pode até ser inédito, contribuindo para garantir que a recolha nos termos da secção 702 ocorre dentro dos limites legais adequados.

([1]) *Id*.

([2]) *Id.*, no ponto 8; 50 U.S.C. § 1881a(l); *ver também NSA Director of Civil Liberties and Privacy Report, «NSA's Implementation of Foreign Intelligence Surveillance Act Section 702»* (em seguida designado «relatório da NSA»), p. 4, *disponível em* http://icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties.

([3]) *Director of National Intelligence 2014 Transparency Report, disponível em* http://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2014.

([4]) Os procedimentos de minimização encontram-se disponíveis em: http://www.dni.gov/files/documents/ppd-28/2014%20NSA%20702%20Minimization%20Procedures.pdf («NSA Minimization Procedures»); http://www.dni.gov/files/documents/ppd-28/2014%20FBI%20702%20Minimization%20Procedures.pdf; e http://www.dni.gov/files/documents/ppd-28/2014%20CIA%20702%20Minimization%20Procedures.pdf.

([5]) *Ver* relatório da NSA, p. 4.

([6]) *Ver, por exemplo*, procedimentos de minimização da NSA, p. 6.

([7]) Os procedimentos relativos à PPD-28 dos serviços de informações encontram-se disponíveis em http://icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties.

([8]) Ver Procedimentos de minimização da NSA; PPD-28, secção 4.

([9]) Ver 50 U.S.C. § 1881(l); *ver igualmente* PCLOB Report, pontos 66-76.

([10]) Ver Avaliação semestral da conformidade com os procedimentos e diretrizes nos termos da secção 702 da *Foreign Intelligence Surveillance Act*, apresentada pelo Procurador-Geral e o diretor dos serviços nacionais de informações, p. 2–3, *disponível em* http://www.dni.gov/files/documents/Semiannual%20Assessment%20of%20Compliance%20with%20procedures%20and%20guidelines%20issued%20pursuant%20to%20Sect%20702%20of%20FISA.pdf.

([11]) Regra 13 do regulamento interno do Foreign Intelligence Surveillance Court, *disponível em* http://www.fisc.uscourts.gov/sites/default/files/FISC%20Rules%20of%20Procedure.pdf.

([12]) Carta do Excelentíssimo Senhor Reggie B. Walton ao Excelentíssimo Senhor Patrick J. Leahy, de 29 de julho de 2013, *disponível em* http://fas.org/irp/news/2013/07/fisc-leahy.pdf.

([13]) *Ver* secção 401 da *Freedom Act*, P.L. 114-23.

O Congresso exerce a supervisão através de relatórios legalmente exigidos apresentados aos *Intelligence and Judiciary Committees*, bem como de reuniões e audições frequentes. Estes incluem um relatório semestral apresentado pelo Procurador-Geral que documenta a utilização da secção 702 e todas as situações de incumprimento ([1]); uma avaliação semestral distinta apresentada pelo Procurador-Geral e o DNI que documenta a conformidade com os procedimentos de orientação e minimização, nomeadamente a conformidade com os procedimentos destinados a garantir que a recolha é efetuada por um motivo de informação externa válido ([2]); e um relatório anual elaborado pelos chefes dos serviços de informações que inclui uma certificação de que a recolha efetuada nos termos da secção 702 continua a produzir informações externas ([3]).

Em suma, a recolha nos termos da secção 702 é autorizada por lei; sob reserva de vários níveis de revisão, supervisão judicial e supervisão; e, tal como o Tribunal da FISA declarou num parecer recentemente desclassificado, «não é realizada de forma maciça nem indiscriminada», «sendo realizada através de decisões de definição de alvos distintas para meios [de comunicação] individuais» ([4]).

III. FREEDOM ACT

A *USA FREEDOM Act*, aprovado em junho de 2015, alterou significativamente as competências de vigilância dos EUA, bem como outras competências no domínio da segurança nacional, e aumentou a transparência pública no que se refere à utilização destas competências e às decisões do Tribunal da FISA, tal como estabelecido abaixo ([5]). A lei assegura que os nossos profissionais no domínio das informações e da aplicação da lei dispõem das competências de que necessitam para proteger a nação, garantindo ainda que a privacidade das pessoas é devidamente protegida quando estas competências são utilizadas. Aumenta a privacidade e as liberdades cívicas, bem como a transparência.

A referida lei proíbe a recolha em larga escala de qualquer documentação, de cidadãos norte-americanos ou de países terceiros, nos termos de várias disposições da FISA ou através da utilização de *National Security Letters*, uma espécie de intimações administrativas permitidas por lei ([6]). Esta proibição engloba especificamente os metadados telefónicos relativos às chamadas entre pessoas nos EUA e pessoas fora dos EUA e englobaria igualmente a recolha de informações ao abrigo do Escudo de Proteção da Privacidade nos termos destas competências. A referida lei exige que o governo baseie qualquer pedido de documentação ao abrigo destas competências num «termo de seleção específico» — um termo que identifique especificamente uma pessoa, conta, endereço ou dispositivo pessoal para que limite, tanto quanto razoavelmente possível, o âmbito das informações solicitadas ([7]). O que precede garante ainda que a recolha para fins de informação é precisamente centrada e orientada.

A referida lei também fez alterações significativas aos processos perante o Tribunal da FISA, que aumentam a transparência e proporcionam garantias adicionais de que a privacidade será protegida. Tal como salientado acima, autorizou a criação de um grupo permanente de advogados com a devida credenciação de segurança especializados em questões de privacidade e liberdades cívicas, recolha de informações, tecnologias de comunicação ou outros domínios relevantes, que podem ser nomeados para comparecer perante o tribunal na qualidade de *amicus curiae* nos processos que envolvam interpretações novas ou significativas da legislação. Estes advogados estão autorizados a apresentar argumentos jurídicos que aumentem a proteção da privacidade individual e das liberdades cívicas, e terão acesso a todas as informações, incluindo informações classificadas, que o tribunal considere necessárias para o exercício das suas funções ([8]).

A referida lei baseia-se na transparência inédita do governo dos EUA sobre as atividades de informações, exigindo que o DNI, em consulta com o Procurador-Geral, desclassifique ou publique um resumo não classificado de cada decisão, despacho, ou parecer emitido pelo Tribunal da FISA ou o *Foreign Intelligence Surveillance Court of Review* (tribunal encarregado de apreciar os recursos relativos aos pedidos e mandatos em matéria de vigilância) que inclua uma construção ou interpretação significativa de qualquer disposição jurídica.

([1]) Ver 50 U.S.C. § 1881f.
([2]) Ver *id*. § 1881a(l)(1).
([3]) Ver *id*. § 1881a(l)(3). Alguns destes relatórios são classificados.
([4]) Mem. *Opinion and Order*, p. 26 (FISC 2014), *disponível em* http://www.dni.gov/files/documents/0928/FISC%20Memorandum%20Opinion%20and%20Order%2026%20August%202014.pdf.
([5]) Ver *Freedom Act* de 2015, Pub. L. N.º 114-23, § 401, 129 Stat. 268.
([6]) Ver *id*. §§ 103, 201, 501. As *National Security Letters* são autorizadas por várias leis e permitem que o FBI obtenha informações constantes de relatórios de crédito, registos financeiros, bem como registos de transações e assinaturas eletrónicas de determinados tipos de empresas, tendo como único objetivo a proteção contra o terrorismo internacional ou atividades de informações clandestinas. *Ver* 12 U. S.C. § 3414; 15 U.S.C. §§ 1681u-1681v; 18 U.S.C. § 2709. Em regra, as *National Security Letters* são utilizadas pelo FBI para recolher informações fundamentais não relativas a conteúdos em fases iniciais de investigações de contrainformação e luta contra o terrorismo — tais como a identidade do assinante de uma conta que pode estar a comunicar com agentes de um grupo terrorista como o ISIS. Os destinatários de uma *National Security Letter* têm o direito de as impugnar em tribunal. *Ver* 18 U.S.C. § 3511.
([7]) Ver *id*.
([8]) Ver *id*. § 401.

Além disso, a referida lei prevê amplas divulgações sobre a recolha nos termos da FISA e os pedidos de *National Security Letters*. Os Estados Unidos devem divulgar anualmente, ao Congresso e ao público, o número de despachos e certificações nos termos da FISA que são solicitadas e recebidas; estimativas do número de cidadãos dos EUA e de países terceiros visados e afetados por vigilância; e o número de nomeações de *amici curiae*, entre outros elementos de informação ([1]). A referida lei exige ainda a comunicação pública adicional pelo governo dos números de pedidos de *National Security Letters* relativos a cidadãos dos EUA e de países terceiros ([2]).

No que se refere à transparência empresarial, a referida lei oferece às empresas um conjunto de opções para a comunicação pública do número agregado de despachos e diretivas nos termos da FISA ou *National Security Letters* que recebem do governo, bem como do número de contas de clientes visadas por estes despachos ([3]). Várias empresas já procederam a tais divulgações, que revelaram o número limitado de clientes cujos registos foram solicitados.

Estes relatórios de transparência empresarial demonstram que os pedidos de informação dos EUA afetam apenas uma fração minúscula de dados. Por exemplo, um relatório de transparência recente de uma grande empresa demonstra que esta recebeu pedidos relacionados com segurança nacional (nos termos da FISA ou de National Security Letters) que afetam menos de 20 000 das suas contas, numa data em que contavam com, pelo menos, 400 milhões de assinantes. Por outras palavras, todos os pedidos relacionados com segurança nacional dos EUA comunicados por esta empresa afetaram menos de 0,005 % dos seus assinantes. Mesmo que cada um desses pedidos fosse referente a dados do «porto seguro», o que, como é evidente, não é o caso, é óbvio que os pedidos são orientados e numa escala adequada, não sendo recolhidos de forma maciça nem indiscriminada.

Por último, embora as leis que autorizam as *National Security Letters* já tenham limitado as circunstâncias nas quais o destinatário de tal carta pode ser impedido de a divulgar, a referida lei prevê ainda que tais requisitos de não divulgação devem ser revistos periodicamente; exigiu que os destinatários de *National Security Letters* sejam notificados sempre que os factos deixem de fundamentar um requisito de não divulgação; e codificou os procedimentos que os destinatários podem utilizar para impugnar os requisitos de não divulgação ([4]).

Em suma, as importantes alterações da *Freedom Act* às competências dos EUA em matéria de informações constituem indícios claros do grande esforço envidado pelos Estados Unidos para colocar a proteção das informações pessoais, da privacidade, das liberdades cívicas e da transparência na vanguarda de todas as práticas de informação dos EUA.

IV. TRANSPARÊNCIA

Para além da transparência estabelecida pela *Freedom Act*, o setor das informações dos EUA fornece ao público muita informação adicional, definindo um exemplo sólido no que diz respeito à transparência nas suas atividades de informação. O setor das informações publicou muitas das suas políticas, procedimentos, decisões do *Foreign Intelligence Surveillance Court* e outros materiais desclassificados, proporcionando um nível de transparência extraordinário. Além disso, o setor das informações aumentou substancialmente a sua divulgação de estatísticas sobre a utilização, por parte do governo, de competências de recolha para efeitos de segurança nacional. Em 22 de abril de 2015, o setor das informações emitiu o seu segundo relatório anual que apresenta estatísticas sobre a frequência com que o governo utiliza estas competências importantes. O ODNI também publicou, no sítio Web do ODNI e no sítio *IC On the Record*, um conjunto de princípios de transparência específicos ([5]) e um plano de execução que traduz os princípios e iniciativas específicas e mensuráveis ([6]). Em outubro de 2015, o diretor dos serviços nacionais de informações estabeleceu que cada serviço de informações deve nomear um *Intelligence Transparency Officer* (agente responsável pela transparência das informações) no âmbito da sua liderança para promover a transparência e liderar iniciativas de transparência ([7]). Esta entidade trabalhará em estreita colaboração com o *Privacy and Civil Liberties Officer* de cada serviço de informações a fim de assegurar que a transparência, a privacidade e as liberdades cívicas continuam a ser prioritárias.

([1]) Ver *id*. § 602.
([2]) Ver *id*.
([3]) Ver *id*. § 603.
([4]) Ver *id*. §§ 502(f)–503.
([5]) Disponível em http://www.dni.gov/index.php/intelligence-community/intelligence-transparency-principles.
([6]) Disponível em http://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/Principles%20of%20Intelligence%20Transparency%20Implementation%20Plan.pdf.
([7]) Ver *id*.

A título de exemplo destes esforços, o *Chief Privacy and Civil Liberties Officer* da NSA divulgou vários relatórios não classificados nos últimos anos, nomeadamente relatórios sobre as atividades ao abrigo da secção 702, o Decreto Executivo n.º 12333 e a *Freedom Act* ([1]). Além disso, o setor das informações trabalha em estreita colaboração com a PCLOB, o Congresso e a comunidade de defesa da privacidade dos EUA para proporcionar uma maior transparência no que se refere às atividades de informações dos EUA, sempre que possível e em conformidade com a proteção de métodos e fontes de informações sensíveis. No seu conjunto, as atividades de informações dos EUA são igualmente ou mais transparentes do que as de qualquer outra nação no mundo e são tão transparentes quanto possível para serem coerentes com a necessidade de proteger métodos e fontes sensíveis.

Para resumir a ampla transparência que existe no que se refere às atividades de informações dos EUA:

— O setor das informações divulgou e publicou em linha milhares de páginas de pareceres judiciais e procedimentos dos organismos que descrevem os requisitos e procedimentos específicos das nossas atividades de informações. Também divulgámos relatórios sobre a conformidade dos serviços de informações com as restrições aplicáveis.

— Os altos funcionários dos serviços de informações falam publicamente com regularidade sobre os papéis e as atividades das suas organizações, nomeadamente apresentando descrições dos regimes de conformidade e das garantias que regulam o seu trabalho.

— O setor das informações divulgou inúmeros documentos adicionais sobre atividades de informações nos termos da nossa *Freedom of Information Act* (lei relativa à liberdade de informação).

— O Presidente emitiu a PPD-28, estabelecendo publicamente restrições adicionais às nossas atividades de informações e o ODNI emitiu dois relatórios públicos sobre a aplicação dessas restrições.

— O setor das informações é atualmente obrigado por lei a divulgar pareceres jurídicos significativos emitidos pelo Tribunal da FISA ou resumos de tais pareceres.

— O governo é obrigado a comunicar anualmente o seu grau de utilização de determinadas competências em matéria de segurança nacional e as empresas também estão autorizadas a fazê-lo.

— A PCLOB emitiu vários relatórios públicos pormenorizados sobre as atividades de informações e continuará a fazê-lo.

— O setor das informações fornece amplas informações classificadas às comissões de supervisão do Congresso.

— O DNI emitiu princípios de transparência para regular as atividades do setor das informações.

Esta ampla transparência continuará a progredir. Quaisquer informações divulgadas publicamente estarão, como é evidente, acessíveis ao *Department of Commerce* e à Comissão Europeia. A reapreciação anual entre o *Department of Commerce* e a Comissão Europeia sobre a aplicação do Escudo de Proteção da Privacidade proporcionará uma oportunidade para a Comissão Europeia debater quaisquer questões manifestadas por novas informações divulgadas, bem como outras questões relativas ao Escudo de Proteção da Privacidade e o seu funcionamento, e compreendemos que o *Department of Transportation* possa, a critério seu, convidar representantes de outros organismos, designadamente do setor das informações, para participar nessa reapreciação. Como é evidente, o que precede alia-se ao mecanismo previsto na PPD-28 para que os Estados-Membros da UE manifestem preocupações relacionadas com a vigilância junto de um funcionário designado do *State Department*.

V. REPARAÇÃO

A legislação dos EUA proporciona várias vias de recurso aos cidadãos que tenham sido objeto de vigilância eletrónica ilegal para efeitos de segurança nacional. Nos termos da FISA, o direito a solicitar reparação num tribunal dos EUA não está limitado aos cidadãos dos EUA. Um cidadão que consiga demonstrar legitimidade para interpor uma ação disporia de vias de recurso para impugnar a vigilância eletrónica ilegal nos termos da FISA. Por exemplo, a FISA permite que as

([1]) Disponível em https://www.nsa.gov/civil_liberties/_files/nsa_report_on_section_702_program.pdf; https://www.nsa.gov/civil_liberties/_files/UFA_Civil_Liberties_and_Privacy_Report.pdf; https://www.nsa.gov/civil_liberties/_files/UFA_Civil_Liberties_and_Privacy_Report.pdf.

pessoas que são objeto de vigilância eletrónica ilegal interponham ações contra funcionários do governo dos EUA nas suas capacidades pessoais com vista a obterem indemnizações pecuniárias, nomeadamente indemnizações de caráter punitivo e honorários de advogados. *Ver* 50 U.S.C. § 1810. As pessoas que consigam determinar a sua legitimidade para interpor uma ação também têm direito a instaurar uma ação civil de indemnização, nomeadamente para cobrir as custas processuais, contra os Estados Unidos, sempre que as informações sobre si obtidas em vigilância eletrónica ao abrigo da FISA tenham sido utilizadas ou divulgadas de forma ilegal e voluntária. *Ver* 18 U.S.C. § 2712. Se o governo tencionar utilizar ou divulgar quaisquer informações obtidas ou decorrentes de vigilância eletrónica de qualquer pessoa lesada nos termos da FISA contra essa pessoa em processos judiciais ou administrativos nos Estados Unidos, deve notificar previamente a sua intenção ao tribunal e à pessoa, que pode contestar a legalidade da vigilância e solicitar a supressão das informações. *Ver* 50 U.S.C. § 1806. Por último, a FISA prevê ainda sanções penais para os cidadãos que procedam ilegalmente a vigilância eletrónica ilegal no aparente cumprimento da lei ou que utilizem ou divulguem intencionalmente informações obtidas através de vigilância ilegal. *Ver* 50 U.S.C. § 1809.

Os cidadãos da UE dispõem de outras vias de recurso contra os funcionários do governo dos EUA em virtude da utilização ou do acesso ilegal a dados por parte do governo, nomeadamente funcionários do governo que violem a lei no decurso do acesso ou da utilização ilegal de informações para alegados objetivos de segurança nacional. A *Computer Fraud and Abuse Act* (lei sobre a criminalidade informática) proíbe o acesso não autorizado intencional (ou a superação do acesso autorizado) para obter informações de uma instituição financeira, um sistema informático do governo dos EUA, ou um computador acedido através da Internet, bem como ameaças de danos a computadores protegidos para efeitos de extorsão ou fraude. *Ver* 18 U.S.C. § 1030. Qualquer pessoa, independentemente da sua nacionalidade, que sofra danos ou perdas devido a uma violação desta lei pode instaurar uma ação contra o infrator (nomeadamente um funcionário do governo), solicitando uma indemnização compensatória e uma injunção ou qualquer outra medida equitativa nos termos da secção 1030(g), independentemente da interposição de uma ação penal, deste que a conduta implique, pelo menos, uma de várias circunstâncias estabelecidas na lei. A *Electronic Communications Privacy Act* (lei relativa à proteção das comunicações eletrónicas privadas — ECPA) regula o acesso do governo às comunicações eletrónicas armazenadas e aos registos de transações e informações de assinantes detidos por terceiros fornecedores de serviços de comunicações. *Ver* 18 U.S.C. §§ 2701-2712. A ECPA autoriza os cidadãos lesados a interporem ações contra funcionários do governo em virtude do acesso ilegal intencional a dados armazenados. A ECPA é aplicável a todas as pessoas independentemente da sua cidadania e as pessoas lesadas podem receber indemnizações e os honorários dos advogados. A *Right to Financial Privacy Act* (RFPA) limita o acesso do governo dos EUA aos registos bancários e de corretagem financeira dos clientes individuais. *Ver* 12 U.S.C. §§ 3401-3422. Nos termos da RFPA, o cliente de um banco ou de uma corretora financeira pode instaurar uma ação contra o governo dos EUA, solicitando uma indemnização legal, efetiva ou punitiva em virtude da obtenção indevida de acesso aos registos do cliente, e a constatação de que tal acesso indevido foi voluntário desencadeia automaticamente uma investigação de possíveis medidas disciplinares contra os funcionários do governo em causa. *Ver* 12 U.S.C. § 3417.

Por último, a *Freedom of Information Act* (FOIA), prevê um meio para que qualquer pessoa possa solicitar o acesso à documentação existente dos organismos federais sobre qualquer tema, sob reserva de determinadas categorias de derrogações. *Ver* 5 U.S.C. § 552(b). Estas incluem limites ao acesso a informações de segurança nacional classificadas, informações pessoais de outras pessoas e informações relativas a investigações das autoridades responsáveis pela aplicação da lei, e são comparáveis às limitações impostas pelas nações com as suas próprias legislações em matéria de acesso à informação. Estas limitações são igualmente aplicáveis a cidadãos norte-americanos e de países terceiros. Os litígios relativos à divulgação de documentação solicitada nos termos da FOIA podem ser objeto de recurso por via administrativa e posteriormente no tribunal federal. O tribunal deve fazer uma determinação de novo sobre se a documentação é devidamente retida, 5 U.S.C. § 552(a)(4)(B), e pode exigir que o governo conceda o acesso à documentação. Em alguns casos, os tribunais anularam afirmações do governo de que a informação deve ser retida como classificada ([1]). Embora não se encontrem disponíveis indemnizações pecuniárias, os tribunais podem emitir uma decisão sobre os honorários do advogado.

VI. CONCLUSÃO

Os Estados Unidos reconhecem que as suas atividades de recolha de informação de origem eletromagnética e outras atividades de informações devem tomar em consideração que todas as pessoas devem ser tratadas com dignidade e respeito, independentemente da sua nacionalidade ou local de residência e que todas as pessoas têm interesses de privacidade legítimos no tratamento das suas informações pessoais. Os Estados Unidos apenas utilizam a informação de origem eletromagnética para fazer progredir os seus interesses em matéria de política externa e segurança nacional e proteger os seus cidadãos e os cidadãos dos seus aliados e parceiros de quaisquer danos. Em suma, o setor das informações não procede à vigilância indiscriminada de ninguém, nomeadamente de cidadãos europeus comuns.

([1]) Ver, por exemplo, *New York Times v. Department of Justice*, 756 F.3d 100 (2d Cir. 2014); *American Civil Liberties Union v. CIA*, 710 F.3d 422 (D.C. Cir. 2014).

A recolha de informação de origem eletromagnética ocorre apenas quando devidamente autorizada e de forma a cumprir na íntegra estas limitações; apenas após se tomar em consideração a disponibilidade de fontes alternativas, designadamente de fontes públicas e diplomáticas; e de forma a atribuir prioridade a alternativas adequadas e viáveis. Além disso, sempre que possível, a obtenção de informação de origem eletromagnética ocorre apenas através da recolha centrada em alvos ou temas de informação externa específicos através da utilização de discriminantes.

A política dos EUA a este respeito foi confirmada na PPD-28. Neste contexto, os serviços de informações dos EUA não dispõem da autoridade jurídica, dos recursos, da capacidade técnica nem da vontade de intercetar todas as comunicações do mundo. Os referidos serviços não leem as mensagens de correio eletrónico de todas as pessoas dos Estados Unidos nem de todas as pessoas do mundo. Em conformidade com a PPD-28, os Estados Unidos asseguram proteções sólidas às informações pessoais dos cidadãos de países terceiros que são recolhidas através de atividades de informação de origem eletromagnética. Tanto quanto possível, em conformidade com a segurança nacional, tal inclui políticas e procedimentos para minimizar a preservação e divulgação de informações pessoais relativas a cidadãos de países terceiros em comparação com as proteções de que os cidadãos norte-americanos beneficiam. Além disso, tal como discutido acima, o regime de supervisão abrangente da autoridade orientada da secção 702 do FISA é inigualável. Por último, a alteração significativa da legislação dos EUA em matéria de informação estabelecida na *Freedom Act* e as iniciativas lideradas pelo ODNI para promover a transparência no setor das informações melhoram em grande medida a privacidade e as liberdades cívicas de todas as pessoas, independentemente da sua nacionalidade.

Queira aceitar a expressão da minha mais elevada consideração,

Robert S. Litt

21 de junho de 2016

Justin S. Antonipillai
Conselheiro
Department of Commerce dos EUA
1401 Constitution Avenue, N.W.
Washington, DC 20230

Ted Dean
Vice-Secretário Adjunto
International Trade Administration
1401 Constitution Avenue, N.W.
Washington, DC 20230

Excelentíssimos Senhores Antonipillai e Dean:

Tenho o prazer de prestar mais informações sobre a forma como os Estados Unidos efetuam recolha de informação de origem eletromagnética em larga escala. Tal como explicado na nota 5 da *Presidential Policy Directive* 28 (PPD-28), a recolha em larga escala é a aquisição de um volume relativamente elevado de informações ou dados de origem eletromagnética em circunstâncias em que o setor das informações não pode utilizar um identificador associado a um objetivo específico (tais como endereços de correio eletrónico ou números de telefone) para centrar a recolha. No entanto, tal não significa que este tipo de recolha é «massiva» ou «indiscriminada». Com efeito, a PPD-28 exige também que «a atividade de recolha de informação de origem eletromagnética deve ser sempre tão seletiva quanto possível». No quadro deste mandato, o setor das informações toma medidas para assegurar que, mesmo quando não é possível utilizar identificadores específicos para tornar seletiva a recolha, os dados a recolher são suscetíveis de conter informações sobre o estrangeiro, que responderão às exigências definidas pelos responsáveis políticos americanos, em conformidade com o procedimento explicado na minha carta anterior, e limitam a quantidade de informações não pertinentes recolhidas.

A título de exemplo, o setor das informações pode ser levado a adquirir informações de origem eletromagnética sobre as atividades de um grupo terrorista que opera numa região de um país do Médio Oriente, que se pensa que possa estar a planear ataques contra países da Europa ocidental, mas sem que se saibam os nomes, números de telefone, endereços de correio eletrónico e outros elementos de identificação das pessoas associadas a esse grupo terrorista. Podemos optar entre centrar-se nesse grupo, mediante a recolha de comunicações de e para essa região, que serão em seguida filtradas e analisadas a fim de identificar as comunicações relacionadas com o referido grupo. Assim, os serviços de informação procurariam reduzir o mais possível o âmbito da recolha de informações. Esta atividade seria considerada como uma recolha «em larga escala», dado que a utilização de discriminantes não é possível, mas não é nem «massiva» nem «indiscriminada»; pelo contrário, seria uma recolha orientada o mais especificamente possível.

Por conseguinte, mesmo quando uma orientação por meio de seletores específicos não é possível, os Estados Unidos não recolhem todas as comunicações de todos meios de comunicação em todo o mundo, mas aplicam filtros e outros instrumentos técnicos para centrar a sua recolha nos canais de comunicação suscetíveis de ter um valor em termos de informações sobre o estrangeiro. Desta forma, as atividades de informação de origem eletromagnética dos Estados Unidos abrangem apenas uma fração das comunicações que circulam na Internet.

Além disso, tal como referido na minha carta anterior, pelo facto de a recolha «em larga escala» implicar um maior risco de recolha de informações não pertinentes, a PPD-28 limita a seis finalidades específicas a utilização que os serviços de informação podem fazer das informações de origem eletromagnética recolhidas desta forma. A PPD-28 e as políticas das agências que a executam impõem igualmente restrições em matéria de conservação e divulgação de dados pessoais adquiridos através das informações de origem eletromagnética, independentemente da forma da recolha — «em larga escala» ou seletiva — e da nacionalidade das pessoas em causa.

Assim, a recolha «em larga escala» praticada pelos serviços de informações não é uma recolha «massiva» ou «indiscriminada», mas implica a utilização de métodos e instrumentos de filtragem, a fim de orientar a recolha sobre o material que responderá às exigências definidas pelos responsáveis políticos dos Estados Unidos em matéria de informações sobre o estrangeiro, reduzindo o mais possível a recolha de informações não pertinentes, e prevendo regras rigorosas para

proteger as informações não pertinentes eventualmente adquiridas. As políticas e procedimentos descritos na presente carta são aplicáveis a todos os tipos de recolha «em larga escala» de informação de origem de eletromagnética, incluindo a recolha em larga escala de comunicações de e para a Europa, sem que esta carta confirme ou negue a realidade de uma recolha deste tipo.

Também pediu informações adicionais sobre a *Privacy and Civil Liberties Oversight Board* (PCLOB) (comissão de controlo da privacidade e das liberdades cívicas) e os inspetores gerais, e sobre as suas competências. A PCLOB é uma agência independente do poder executivo. Os cinco membros desta comissão bipartida são nomeados pelo Presidente dos Estados Unidos e confirmados pelo Senado ([1]). Cada membro da comissão tem um mandato de seis anos. Os membros da comissão e o seu pessoal beneficiam de habilitações de segurança que lhes permitem executar plenamente as suas funções e responsabilidades legais ([2]).

A missão da PCLOB consiste em assegurar que os esforços envidados pelo Governo federal para prevenir o terrorismo são equilibrados com a necessidade de proteção da privacidade e das liberdades cívicas. A comissão tem duas responsabilidades fundamentais — supervisão e o conselho. A PCLOB define o seu próprio programa de trabalho e determina as atividades de supervisão ou de conselho que pretende realizar.

No seu papel de *supervisão*, a PCLOB examina e analisa as medidas tomadas pelo poder executivo com vista a proteger o país do terrorismo, assegurando que a necessidade de tais medidas é compensada pela necessidade de proteger a privacidade e as liberdades cívicas ([3]). O exame mais recente completado foi consagrado aos programas de vigilância executados nos termos da secção 702 da FISA ([4]), estando atualmente a conduzir um exame das atividades de informação realizadas nos termos do Decreto de 12333 ([5]).

Na sua função *consultiva*, a PCLOB garante que a elaboração e execução das leis, regulamentos e políticas relativas aos esforços para proteger o país do terrorismo tenham devidamente em conta as questões ligadas às liberdades ([6]).

A fim de desempenhar as suas funções, a comissão está autorizada por lei a aceder a todos os registos, relatórios, auditorias, análises, documentos, papéis, recomendações e quaisquer outros documentos pertinentes das agências, incluindo as informações classificadas nos limites previstos pela lei ([7]). Além disso, a comissão pode interrogar, recolher o depoimento ou o testemunho público de qualquer funcionário ou dependente do poder executivo ([8]). Por outro lado, a comissão pode solicitar por escrito que o *Attorney General* (Procurador-Geral) emita, em nome da comissão, citações de comparência para obrigar as partes que não pertencem ao poder executivo a prestar informações de interesse ([9]).

Por último, a PCLOB está estatutariamente sujeita a exigências de transparência pública. Tal inclui manter o público informado das suas atividades, através da realização de audições públicas e de tornar os seus relatórios acessíveis ao público, compatibilizando na medida possível, estas exigências com a proteção de informações classificadas ([10]). Além disso, a comissão é obrigada a comunicar quando uma entidade do poder executivo se recusou a seguir o seu parecer.

Os inspetores gerais (IG) dentro dos serviços de informação (*Intelligence Community* — IC) realizam auditorias, inspeções e avaliações dos programas e atividades neste setor para identificar e tratar os riscos sistémicos, as vulnerabilidades e deficiências. Além disso, os IG investigam as queixas ou alegações de violação da legislação ou da regulamentação, ou de

([1]) 42 U.S.C. 2000ee(a), (h).
([2]) 42 U.S.C. 2000ee(k).
([3]) 42 U.S.C. 2000ee(d)(2).
([4]) Ver em geral https://www.pclob.gov/library.html#oversightreports.
([5]) Ver em geral https://www.pclob.gov/events/2015/may13.html.
([6]) 42 U.S.C. 2000ee(d)(1); ver igualmente *PCLOB Advisory Function Policy and Procedure, Policy* 2015-004, disponível em https://www.pclob.gov/library/Policy-Advisory_Function_Policy_Procedure.pdf.
([7]) 42 U.S.C. 2000ee(g)(1)(A).
([8]) 42 U.S.C. 2000ee(g)(1)(B).
([9]) 42 U.S.C. 2000ee(g)(1)(D).
([10]) 42 U.S.C. 2000eee(f).

má gestão; de desperdício elevado de fundos; de abuso de autoridade ou de ameaça concreta e específica para a saúde e segurança públicas decorrente de programas ou de atividades dos serviços de informações. A independência dos IG é uma componente essencial para a objetividade e a integridade de cada relatório, conclusão e recomendação emitida por um IG. O processo de nomeação e de revocação dos IG, a separação das competências operacionais, orçamentais e em matéria de pessoal; e a dupla exigência de reportar aos responsáveis pela entidade do poder executivo e do Congresso, entre outros aspetos, formam a pedra angular sobre a qual assenta a independência dos IG.

O Congresso criou um gabinete independente dos IG em cada entidade do poder executivo, incluindo cada componente dos serviços de informação ([1]). Com a promulgação da *Intelligence Authorization Act for Fiscal Year 2015*, quase todos os IG que exercem a supervisão sobre um serviço da IC são nomeados pelo Presidente e confirmados pelo Senado, incluindo o *Department of Justice*, a *Central Intelligence Agency*, a *National Security Agency*, e a *Intelligence Community* ([2]). Além disso, estes IG são funcionários apartidários, admitidos a tempo indeterminado e apenas o Presidente os pode destituir do cargo. Embora a Constituição dos Estados Unidos preveja esta faculdade, o Presidente exerceu-a raramente; tal faculdade impõe igualmente que o Presidente transmita ao Congresso uma fundamentação escrita 30 dias antes da destituição do cargo do IG ([3]). O procedimento estabelecido assegura que os agentes do poder executivo não exerçam qualquer influência indevida sobre a escolha, nomeação e destituição dos IG.

Em segundo lugar, a lei confere aos IG competências significativas para o exercício de auditorias, investigações e verificações dos programas e operações do poder executivo. Para além da supervisão das investigações e verificações prevista pela lei, os IG têm uma ampla margem de manobra para exercer o poder de supervisão para analisar programas e atividades da sua escolha ([4]). No exercício deste poder, a lei assegura aos IG os recursos independentes para desempenhar as suas funções, incluindo o poder de recrutar o seu próprio pessoal e de documentar separadamente os seus pedidos orçamentais ao Congresso ([5]). A lei garante aos IG o acesso às informações necessárias para desempenhar as suas funções. Tal inclui o poder de aceder diretamente a todos os dados e informações relativos aos programas e operações da entidade, independentemente da sua classificação; o poder de ordenar a apresentação de informações e documentos; e o poder de recolher testemunhos ([6]). Num número limitado de casos, o responsável por uma entidade do poder executivo, pode proibir uma determinada atividade do IG, se, por exemplo, uma auditoria ou investigação do IG é suscetível de comprometer significativamente os interesses da segurança nacional dos Estados Unidos. Também neste caso, este poder é exercido muito raramente e implica que o responsável pela entidade tenha de notificar o Congresso no prazo de 30 dias das razões para o seu exercício ([7]). Com efeito, o diretor dos serviços nacionais de informação nunca exerceu este poder de limitação sobre qualquer atividade dos IG.

Em terceiro lugar, os IG têm a missão de manter os diretores das entidades do poder executivo e o Congresso plenamente e constantemente informados, através de relatórios, de fraude e de outros problemas graves, de abusos e das deficiências relacionadas com os programas e atividades do poder executivo ([8]). A obrigação de reportar aos dois ramos reforça a independência dos IG, assegurando a transparência dos seu procedimentos de supervisão e oferecendo aos diretores das entidades a possibilidade de aplicar as suas recomendações antes que o Congresso possa tomar medidas legislativas. Por exemplo, os IG são obrigados por lei a elaborar relatórios semestrais que indicam os problemas encontrados, bem como as medidas corretivas adotadas até à data ([9]). As entidades do poder executivo tomam

([1]) Secções 2 e 4 da *Inspector General Act* de 1978, tal como alterado (a seguir «IG Act»); Secção 103H(b) e (e) da *National Security Act* de 1947, tal como alterado (a seguir «Nat'l Sec. Act»); Secção 17(a) da *Central Intelligence Act* (a seguir «CIA Act»).

([2]) Ver Pub. L. N.º 113-293, 128 Stat. 3990, (19 de dezembro de 2014). Os IG da *Defense Intelligence Agency* e da *National Geospatial--Intelligence Agency* não são nomeados pelo Presidente; no entanto, o DOD IG e o IC IG têm jurisdição concorrente sobre essas agências.

([3]) Secção 3 da *IG Act* de 1978, tal como alterado; Secção 103H(c) da *Nat'l Sec. Act*; e Secção 17(b) da *CIA Act*.

([4]) Ver secções 4(a) e 6(a)(2) da *IG Act* de 1947; secção 103H(e) e (g)(2)(A) da *Nat'l Sec. Act*; secção 17(a) e (c) da *CIA Act*.

([5]) Secções 3(d), 6(a)(7) e 6(f) da *IG Act*; secções 103H(d), (i), (j) e (m) da *Nat'l Sec. Act*; secções 17(e)(7) e (f) da *CIA Act*.

([6]) Secção 6(a)(1), (3), (4), (5), e (6) da *IG Act*; secções 103H(g)(2) da *Nat'l Sec. Act*; secção 17(e)(1), (2), (4), e (5) da *CIA Act*.

([7]) Ver, por exemplo, secções 8(b) e 8E(a) da *IG Act*; secção 103H(f) da *Nat'l Sec. Act*; secção 17(b) da *CIA Act*.

([8]) Secção 4(a)(5) da *IG Act*; secção 103H(a)(b)(3) e (4) da *Nat'l Sec. Act*; secção 17(a)(2) e (4) da *CIA Act*.

([9]) Secção 2(3), 4(a), e 5 da *IG Act*; secção 103H(k) da *Nat'l Sec. Act*; secção 17(d) da *CIA Act*. Os relatórios que o Inspector-General do *Department of Justice* tornou públicos estão disponíveis na Internet em: http://oig.justice.gov/reports/all.htm. Do mesmo modo, o Inspetor-Geral da *Intelligence Community* publica os seus relatórios semestrais em: https://www.dni.gov/index.php/intelligence-community/ic-policies-reports/records-requested-under-foia#icig.

seriamente em consideração as conclusões e recomendações dos IG e é frequente que incluam a aceitação e a aplicação, por parte destas entidades, das recomendações dos IG nos referidos relatórios semestrais e noutros relatórios apresentados ao Congresso e, em alguns casos, tornados públicos ([1]). Para além desta estrutura de duplo reporte, os IG são igualmente encarregados de acompanhar os denunciantes dentro do poder executivo quando estes decidem divulgar às comissões de supervisão do Congresso competentes fraudes, desperdícios, ou abusos nos programas e atividades do poder executivo. Os denunciantes têm a garantia de que a sua identidade não será revelada ao poder executivo, o que os põe ao abrigo de eventuais medidas proibidas de represália de ordem profissional ou que atingem a sua habilitação de segurança, pelo facto de ter comunicado informações aos IG ([2]). Dado que os denunciantes estão muitas vezes na origem de investigações realizadas pelos IG, a possibilidade de revelar as suas preocupações ao Congresso sem interferência do poder executivo reforça a eficácia da vigilância realizada pelos IG. Em razão desta independência, os IG podem promover o progresso da economia, da eficiência e da responsabilização nas entidades do poder executivo com objetividade e integridade.

Por último, Congresso criou o Conselho dos Inspetores-Gerais a favor da integridade e da eficácia (*Council of Inspectors General on Integrity and Efficiency*). Este conselho, entre outras atividades, elabora as normas para as auditorias, as investigações e as verificações do IG; promove a formação; e tem a competência para realizar investigações sobre a alegada má conduta dos IG, exercendo assim uma análise crítica sobre os IG, que são os responsáveis pela vigilância dos outros ([3]).

Esperando que esta informação lhe possa ser útil,

queira aceitar os protestos da minha mais elevada consideração,

Robert S. Litt

Conselheiro-Geral

([1]) Secção 2(3), 4(a), e 5 da *IG Act*; secção 103H(k) da *Nat'l Sec. Act*; secção 17(d) da *CIA Act*. Os relatórios que o Inspector-Geral do *Department of Justice* tornou públicos estão disponíveis na Internet em: http://oig.justice.gov/reports/all.htm. Do mesmo modo, o Inspetor-Geral da *Intelligence Community* publica os seus relatórios semestrais em: https://www.dni.gov/index.php/intelligence-community/ic-policies-reports/records-requested-under-foia#icig.

([2]) Secção 7 da *IG Act*; secção 103H(g)(3) da *Nat'l Sec. Act*; secção 17(e)(3) da *CIA Act*.

([3]) Secção 11 da *IG Act*.

ANEXO VII

Carta do Vice-Procurador-Geral Adjunto e Conselheiro para os Assuntos Internacionais, Bruce Swartz, *Department of Justice* dos EUA

19 de fevereiro de 2016

Justin S. Antonipillai
Conselheiro
Department of Commerce dos EUA
1401 Constitution Ave, NW
Washington, DC 20230

Ted Dean
Vice-Secretário Adjunto
International Trade Administration
1401 Constitution Ave, NW
Washington, DC 20230

Excelentíssimos Senhores Antonipillai e Dean:

A presente carta apresenta uma breve visão geral dos principais instrumentos de investigação utilizados para obter dados comerciais e outras informações sobre documentação de empresas nos Estados Unidos para efeitos de aplicação do direito penal ou para efeitos (civis e regulamentares) de interesse público, nomeadamente das limitações ao acesso estipuladas nessas competências ([1]). Estes processos jurídicos são não discriminatórios desde que sejam utilizados para obter informações de empresas nos Estados Unidos, designadamente de empresas que autocertificarão a sua adesão através do quadro do Escudo de Proteção da Privacidade, sem tomar em consideração a nacionalidade do titular dos dados. Além disso, as empresas que são objeto de um processo jurídico nos Estados Unidos podem impugná-lo em tribunal, tal como debatido abaixo ([2]).

A Quarta Emenda da Constituição dos Estados Unidos é de especial importância no que diz respeito à apreensão de dados pelas autoridades públicas, uma vez que prevê que «[o] direito do povo à inviolabilidade das suas pessoas, casas, documentos e haveres contra buscas e apreensões arbitrárias não poderá ser infringido, e nenhum mandado será emitido, salvo com base numa causa provável, apoiada por juramento ou declaração, e nomeadamente com a descrição do local da busca e das pessoas ou coisas a apreender». (Quarta Emenda da Constituição dos EUA). Tal como o Supremo Tribunal dos EUA declarou em *Berger v. State of New York*, «[a] finalidade básica desta emenda, tal como reconhecida em inúmeras decisões deste Tribunal, consiste em salvaguardar a privacidade e a segurança das pessoas contra invasões arbitrárias pelos funcionários do governo». 388 U.S. 41, 53 (1967) (*citando Camara v. Mun. Court of San Francisco*, 387 U. S. 523, 528 (1967)). Em regra, nas investigações penais nacionais, a Quarta Emenda exige que os agentes responsáveis pela aplicação da lei obtenham um mandado emitido pelo tribunal antes da realização de uma busca. *Ver Katz v. United States*, 389 U.S. 347, 357 (1967). Sempre que o requisito de mandado não seja aplicável, a atividade do governo é objeto de um teste de «razoabilidade» ao abrigo da Quarta Emenda. Portanto, a própria Constituição garante que o governo dos EUA não dispõe de competências ilimitadas ou arbitrárias para apreender informações privadas.

Autoridades responsáveis pela aplicação do direito penal:

Os procuradores federais, que são funcionários do *Department of Justice* (DOJ) e os agentes federais de investigação, nomeadamente os agentes do *Federal Bureau of Investigation* (Gabinete Federal de Investigação — FBI), um organismo do DOJ responsável pela aplicação da lei, têm competência para exigir a apresentação de documentos e outras informações

([1]) A presente visão geral não descreve os instrumentos de investigação da segurança nacional utilizados pelas autoridades responsáveis pela aplicação da lei no terrorismo e noutras investigações em matéria de segurança nacional, nomeadamente *National Security Letters* (cartas de segurança nacional — NSL) para determinadas informações de documentação em relatórios de crédito, registos financeiros e registos de transações e assinaturas eletrónicas, ver 12 U.S.C. § 3414; 15 U.S.C. § 1681u; 15 U.S.C. § 1681v; 18 U.S.C. § 2709, e, no que diz respeito à vigilância eletrónica, mandados de busca, documentação empresarial e outra recolha de comunicações nos termos da *Foreign Intelligence Surveillance Act* (lei relativa à vigilância dos serviços de informações externas), ver 50 U.S.C. § *et seq*.

([2]) O presente documento debate as competências regulamentares e de aplicação da legislação federal; as violações da legislação estadual são investigadas pelos Estados e são apreciadas em tribunais estaduais. As autoridades estaduais responsáveis pela aplicação da lei utilizam mandados e intimações emitidos ao abrigo do direito estadual essencialmente da forma aqui descrita, mas com a possibilidade de o processo judicial estadual ser objeto de proteções previstas pelas constituições estaduais que ultrapassam as da Constituição dos EUA. As proteções da legislação estadual devem ser pelo menos equivalentes às da Constituição dos EUA, incluindo, entre outras, a Quarta Emenda.

de registos de empresas nos Estados Unidos para efeitos de investigação penal através de vários tipos de processos jurídicos obrigatórios, nomeadamente intimações emitidas por um júri, intimações administrativas e mandados de busca, e podem obter outras comunicações ao abrigo das competências federais penais em matéria de escutas e dispositivos de registo de chamadas telefónicas e comunicações eletrónicas.

Intimações emitidas por um júri ou para um julgamento: As intimações penais são utilizadas para apoiar investigações orientadas em matéria de aplicação da lei. Uma intimação de um júri consiste num pedido oficial emitido por um júri (normalmente mediante pedido de um procurador federal) para apoiar a investigação realizada por um júri sobre uma suspeita de violação do direito penal específica. Os júris constituem um ramo de investigação do tribunal e são nomeados por um juiz ou magistrado. Uma intimação pode exigir que alguém apresente um depoimento numa ação, ou apresente ou disponibilize documentação empresarial, informações eletronicamente armazenadas ou outros elementos tangíveis. As informações devem ser relevantes para a investigação e a intimação não pode ser pouco razoável em virtude ser demasiado abrangente, opressiva ou onerosa. Um destinatário pode apresentar uma moção para contestar a intimação com base nesses motivos. *Ver* Fed. R. Crim. p. 17. Em circunstâncias limitadas, as intimações para um julgamento respeitantes a documentos podem ser utilizadas após o júri ter efetuado a acusação.

Competência de intimação administrativa: As competências de intimação administrativa podem ser exercidas em investigações penais ou civis. No contexto da aplicação do direito penal, várias leis federais autorizam a utilização de intimações administrativas para a apresentação ou disponibilização de documentação empresarial, informações eletronicamente armazenadas ou outros elementos tangíveis em investigações relativas a casos de fraude nos serviços de saúde, abuso de crianças, proteção dos serviços secretos, substâncias controladas e investigações dos inspetores-gerais que impliquem organismos do governo. Se o governo procurar executar uma intimação administrativa em tribunal, o seu destinatário, a par do destinatário de uma intimação emitida por um júri, pode alegar que a intimação não é razoável em virtude de ser demasiado abrangente, opressiva ou onerosa.

Decisões judiciais relativas a dispositivos de registo de chamadas telefónicas e comunicações eletrónicas: Nos termos das disposições em matéria de dispositivos de registo de chamadas telefónicas e comunicações eletrónicas, as autoridades responsáveis pela aplicação da lei podem obter uma decisão judicial para a obtenção de informações em tempo real, não relativas a conteúdo sobre a marcação, o encaminhamento, o endereçamento e a sinalização relativas a um número de telefone ou endereço de correio eletrónico após a certificação de que as informações fornecidas são relevantes para uma investigação penal em curso. *Ver* 18 U.S.C. §§ 3121-3127. A utilização ou instalação de tal dispositivo à margem da lei constitui um crime federal.

Electronic Communications Privacy Act (lei relativa à proteção das comunicações eletrónicas privadas — ECPA): Existem regras adicionais que regulam o acesso do governo às informações sobre assinantes, aos dados de tráfego e ao conteúdo armazenado de comunicações detidos pelas empresas telefónicas que prestam serviços de Internet e outros prestadores de serviços, nos termos do título II da ECPA, igualmente denominada *Stored Communications Act* (SCA), 18 U.S.C. §§ 2701–2712. A SCA estabelece um sistema de direitos legais em matéria de privacidade que limitam o acesso das autoridades responsáveis pela aplicação da lei aos dados para além do que é necessário ao abrigo do direito constitucional dos clientes e assinantes de fornecedores de serviços de Internet. A SCA prevê níveis crescentes de proteções da privacidade em função do caráter intrusivo da recolha. Para obter acesso às informações de registo dos assinantes, a endereços IP e aos carimbos temporais associados, bem como a informações sobre faturação, as autoridades responsáveis pela aplicação do direito penal devem obter uma intimação. No que diz respeito à restante informação armazenada não relativa ao conteúdo, tal como o cabeçalho de mensagens de endereço eletrónico sem o título, a autoridade responsável pela aplicação da lei deve apresentar factos específicos a um juiz que demonstrem que as informações solicitadas são relevantes e significativas para uma investigação penal em curso. Para obter o conteúdo armazenado de comunicações eletrónicas, em geral, as autoridades responsáveis pela aplicação do direito penal obtêm um mandado de um juiz com base numa causa provável para considerar que a conta em questão contém provas de um crime. A SCA prevê igualmente a responsabilidade civil e sanções penais.

Decisões judiciais relativas a vigilância nos termos da *Federal Wiretap Law*: Além disso, as autoridades responsáveis pela aplicação da lei podem intercetar comunicações eletrónicas, orais ou por cabo em tempo real para efeitos de investigação penal nos termos da lei federal relativa às escutas. *Ver* 18 U.S.C. §§ 2510-2522. Esta competência encontra-se disponível apenas nos termos de uma decisão judicial na qual um juiz considere, designadamente, que existe uma

causa provável para considerar que a escuta ou interceção eletrónica produzirá provas de um crime federal ou a localização de um fugitivo. A lei prevê responsabilidade civil e sanções penais por violações das disposições em matéria de escutas.

Mandado de busca — regra 41: As autoridades responsáveis pela aplicação da lei podem realizar buscas físicas nos Estados Unidos sempre que um juiz o autorize. As autoridades responsáveis pela aplicação da lei devem demonstrar ao juiz, com base na apresentação de uma «causa provável» de que um crime foi cometido ou está prestes a ser cometido e de que os elementos relacionados com o crime serão provavelmente encontrados no local especificado pelo mandado. Esta competência é muitas vezes utilizada sempre que uma busca física a instalações pela polícia seja necessária devido ao perigo de destruição de provas caso uma intimação ou outra decisão de apresentação de documentos seja notificada à empresa. Ver Quarta Emenda da Constituição dos EUA (debatida em maior pormenor acima, Fed. R. Crim. p. 41. O alvo de um mandado de busca pode tentar anular o mandado por ser demasiado abrangente, abusivo ou indevidamente obtido e as partes lesadas com legitimidade podem solicitar a supressão de quaisquer provas obtidas numa busca ilegal. Ver *Mapp v. Ohio*, 367 U.S. 643 (1961).

Diretrizes e políticas do DOJ: Para além destas limitações constitucionais, jurídicas e com base em regras ao acesso do governo aos dados, o Procurador-Geral emitiu diretrizes que estipulam limites adicionais ao acesso das autoridades responsáveis pela aplicação da lei aos dados e que contêm igualmente proteções relativas à privacidade e às liberdades cívicas. Por exemplo, as diretrizes do Procurador-Geral para as operações nacionais do FBI (*Attorney General's Guidelines for Domestic Federal Bureau of Investigation (FBI) Operations*) (setembro de 2008) (em seguida designadas «diretrizes do Procurador-Geral para o FBI»), disponíveis em http://www.justice.gov/archive/opa/docs/guidelines.pdf, estabelecem limites à utilização de meios de investigação para procurar informações relacionadas com investigações que impliquem crimes federais. Estas diretrizes exigem que o FBI utilize os métodos de investigação menos invasivos possíveis, tomando em consideração o efeito sobre a privacidade e as liberdades cívicas, bem como os potenciais danos à reputação. Além disso, salientam que «é axiomático que o FBI realize as suas investigações e outras atividades de uma forma legítima e razoável que respeite a liberdade e a privacidade e evite invasões desnecessárias das vidas das pessoas respeitadoras da lei». *Ver* diretrizes do Procurador-Geral para o FBI, p. 5. O FBI implementou estas diretrizes através do guia do FBI para as operações e investigações nacionais (*FBI Domestic Investigations and Operations Guide* — DIOG), disponível em https://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20(DIOG), um manual abrangente que inclui limites pormenorizados à utilização de instrumentos de investigação e orientações para garantir que as liberdades cívicas e a privacidade são protegidas em todas as investigações. As regras e políticas adicionais que prescrevem limitações às atividades de investigação dos procuradores federais encontram-se estabelecidas no **United States Attorneys' Manual** (USAM), também disponível em linha em http://www.justice.gov/usam/united-states-attorneys-manual.

Competências civis e regulamentares (interesse público):

Também existem limites significativos ao acesso regulamentar ou civil (*isto é*, «interesse público») aos dados detidos por empresas nos Estados Unidos. Os organismos com responsabilidades civis e regulamentares podem emitir intimações a empresas para a obtenção de documentação empresarial, informações eletronicamente armazenadas ou outros elementos tangíveis. Estes organismos encontram-se limitados no exercício da sua competência em matéria de intimações administrativas ou civis não apenas pelas suas leis orgânicas, mas também pelo controlo judicial independente das intimações antes da potencial execução judicial. Ver, por exemplo, Fed. R. Civ. p. 45. Os organismos podem solicitar o acesso apenas aos dados relevantes para questões no âmbito da sua competência de regulamentação. Além disso, o destinatário de uma intimação administrativa pode contestar a execução dessa intimação em tribunal através da apresentação de provas de que o organismo não agiu em conformidade com as normas básicas de razoabilidade, tal como debatido previamente.

Existem outras bases jurídicas que as empresas podem invocar para impugnar os pedidos de dados de organismos administrativos com base nos seus setores específicos e nos tipos de dados de que dispõem. Por exemplo, as instituições financeiras podem impugnar as intimações administrativas que solicitem determinados tipos de informações como violações da *Bank Secrecy Act* (lei relativa ao sigilo bancário) e dos respetivos regulamentos de execução. Ver 31 U.S.C. § 5318, 31 C.F.R. Part X. Outras empresas podem basear-se na *Fair Credit Reporting Act*, ver 15 U.S.C. § 1681b, ou um conjunto de outras leis específicas de setores. A utilização abusiva da competência de um organismo em matéria de intimações pode resultar na sua responsabilidade ou na responsabilidade pessoal dos funcionários do organismo. Ver, por exemplo, *Right to Financial Privacy Act*, 12 U.S.C. §§ 3401–3422. Assim, os tribunais dos Estados Unidos são os guardiões contra pedidos regulamentares indevidos e proporcionam a supervisão independente das ações dos organismos federais.

Por último, qualquer poder regulamentar que as autoridades administrativas tenham para apreender fisicamente a documentação de uma empresa nos Estados Unidos nos termos de uma busca administrativa deve cumprir os requisitos da Quarta Emenda. *Ver See v. City of Seattle*, 387 U.S. 541 (1967).

Conclusão

Todas as atividades regulamentares e de aplicação da lei nos Estados Unidos devem respeitar a legislação aplicável, nomeadamente a Constituição, as leis, as normas e os regulamentos dos EUA. Tais atividades também devem observar as políticas relevantes, nomeadamente as diretrizes do Procurador-Geral que regulam as atividades de aplicação do direito federal. O quadro jurídico descrito acima limita a capacidade dos organismos regulamentares e responsáveis pela aplicação da lei dos EUA de obterem informações de empresas nos Estados Unidos — quer as informações digam respeito a cidadãos norte-americanos ou de países estrangeiros — e, além disso, permite o controlo judicial de quaisquer pedidos de dados por parte do governo nos termos destas competências.

Queira aceitar a expressão da minha mais elevada consideração,

Bruce C. Swartz

Vice-Procurador-Geral Adjunto e Conselheiro para os Assuntos Internacionais