DECISÃO DE EXECUÇÃO (UE) 2023/1795 DA COMISSÃO

de 10 de julho de 2023

nos termos do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho sobre a adequação do nível de proteção dos dados pessoais no âmbito Quadro de Privacidade de Dados UE-EUA

[notificada com o número C(2023) 4745]

(Texto relevante para efeitos do EEE)

A COMISSÃO EUROPEIA,

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

Tendo em conta o 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) ([1]), nomeadamente o artigo 45.º, n.º 3,

Considerando o seguinte:

1. INTRODUÇÃO

(1) O Regulamento (UE) 2016/679 ([2]) estabelece as regras relativas à transferência de dados pessoais para países terceiros e organizações internacionais pelos responsáveis pelo tratamento e subcontratantes na União, na medida em que essa transferência seja abrangida pelo respetivo âmbito de aplicação. As regras relativas às transferências internacionais de dados são definidas no capítulo V do referido regulamento. Embora a circulação de dados pessoais com origem e destino a países não pertencentes à União Europeia seja essencial para o desenvolvimento do comércio transfronteiriço e da cooperação internacional, é indispensável garantir que o nível de proteção conferido aos dados pessoais na União não é comprometido por transferências para países terceiros ou organizações internacionais ([3]).

(2) Nos termos do artigo 45.º, n.º 3, do Regulamento (UE) 2016/679, a Comissão pode decidir, através de um ato de execução, que um país terceiro, um território ou um ou mais setores específicos de um país terceiro garante um nível de proteção adequado. Nessa condição, as transferências de dados pessoais para um país terceiro podem realizar-se sem que para tal seja necessária mais nenhuma autorização, conforme previsto no artigo 45.º, n.º 1, e no considerando 103 do Regulamento (UE) 2016/679.

(3) Conforme estabelecido no artigo 45.º, n.º 2, do Regulamento (UE) 2016/679, a adoção de uma decisão de adequação deve basear-se numa análise exaustiva da ordem jurídica do país terceiro, que abranja tanto as regras aplicáveis a importadores de dados como as limitações e garantias relativas ao acesso aos dados pessoais pelas autoridades públicas. Na sua avaliação, a Comissão tem de apurar se o país terceiro em causa garante um nível de proteção «essencialmente equivalente» ao assegurado na União [considerando 104 do Regulamento (UE) 2016/679]. A questão de saber se é esse o caso deve ser apreciada à luz da legislação da União Europeia, nomeadamente pelo Regulamento (UE) 2016/679, bem como pela jurisprudência do Tribunal de Justiça da União Europeia (o Tribunal de Justiça) ([4]).

([1]) OJ L 119, 4.5.2016, p. 1.
([2]) A fim de facilitar as referências, o anexo VIII inclui uma lista das abreviaturas utilizadas na presente decisão.
([3]) Ver considerando 101 do Regulamento (UE) 2016/679.
([4]) Ver, mais recentemente, o acórdão do Tribunal de Justiça de 16 de julho de 2020, Facebook Ireland e Schrems («Schrems II»), C-311/18, ECLI:EU:C:2020:559.

(4) Conforme esclareceu o Tribunal de Justiça no seu Acórdão de 6 de outubro de 2015, Data Protection Commissioner ([5]) («Schrems»), C-362/14, ECLI:EU:C:2015:650, não é exigido um nível de proteção idêntico. Mais concretamente, os meios a que o país terceiro em causa recorre para proteger os dados pessoais podem ser diferentes dos aplicados na União, desde que se revelem, na prática, eficazes para assegurar um nível adequado de proteção ([6]). Por conseguinte, o padrão de adequação não exige que as regras da União sejam replicadas ponto por ponto. Em vez disso, importa aferir sobretudo se, por meio do teor dos direitos de privacidade e da sua aplicação, controlo e execução efetivos, o sistema estrangeiro consegue, no seu conjunto, garantir o nível de proteção exigido ([7]). Além disso, segundo esse acórdão, ao aplicar esta norma, a Comissão deve avaliar, nomeadamente, se o quadro jurídico do país terceiro em causa prevê normas destinadas a limitar ingerências nos direitos fundamentais dos cidadãos cujos dados são transferidos da União, ingerências essas que as autoridades estatais deste país seriam autorizadas a praticar quando prosseguem objetivos legítimos, tais como a segurança nacional, e se prevê uma proteção jurídica eficaz contra ingerências dessa natureza ([8]). O «documento de referência» relativo à adequação do Comité Europeu para a Proteção de Dados, que procura clarificar esta norma, também fornece orientações a este respeito ([9]).

(5) A norma aplicável no que diz respeito a essa ingerência nos direitos fundamentais à privacidade e à proteção de dados foi clarificada pelo Tribunal de Justiça no seu acórdão de 16 de julho de 2020, Data Protection Commissioner/Facebook Ireland Ltd e Maximillian Schrems («Schrems II»), C-311/18, que declarou inválida a Decisão de Execução (UE) 2016/1250 da Comissão ([10]) relativa a um anterior quadro transatlântico de fluxo de dados, o Escudo de Proteção da Privacidade UE-EUA (Escudo de Proteção da Privacidade). O Tribunal de Justiça considerou que as limitações da proteção de dados pessoais que decorrem da regulamentação interna dos Estados Unidos relativa ao acesso e à utilização, pelas autoridades públicas americanas, desses dados transferidos da União para os Estados Unidos não estavam enquadradas de forma a satisfazer os requisitos substancialmente equivalentes aos exigidos no direito da União, no que diz respeito à necessidade e à proporcionalidade dessas ingerências no direito à proteção de dados ([11]). O Tribunal de Justiça também considerou que não existia qualquer via de recurso num órgão que proporcionasse aos cidadãos cujos dados eram transferidos para os Estados Unidos garantias substancialmente equivalentes às exigidas no artigo 47.º da Carta relativo ao direito à ação e a um tribunal imparcial ([12]).

(6) Na sequência do acórdão Schrems II, a Comissão encetou conversações com o Governo dos EUA com vista a uma possível nova decisão de adequação que cumprisse os requisitos do artigo 45.º, n.º 2, do Regulamento (UE) 2016/679, tal como interpretado pelo Tribunal de Justiça. Em resultado destas conversações, os Estados Unidos adotaram, em 7 de outubro de 2022, o *Executive Order 14086* intitulado «Enhancing Safeguards for [US] Signals Intelligence Activities» (EO 14086), que é complementado por um regulamento relativo ao *Data Protection Review Court* emitido pelo *Attorney General* dos EUA (Regulamento AG) ([13]). Além disso, o quadro aplicável às entidades comerciais responsáveis pelo tratamento de dados da União no âmbito da presente decisão — o «Quadro de Privacidade de Dados UE-EUA» (QPD UE-EUA ou QPD) — foi atualizado.

(7) A Comissão analisou cuidadosamente a legislação e a prática dos EUA, nomeadamente o EO 14086 e o Regulamento AG. Com base nas conclusões estabelecidas nos considerandos 9-200, a Comissão conclui que os EUA asseguram um nível de proteção adequado dos dados pessoais transferidos ao abrigo do QPD UE-EUA de um responsável pelo tratamento ou de um subcontratante na União ([14]) para organizações certificadas nos Estados Unidos.

([5]) Acórdão do Tribunal de Justiça de 6 de outubro de 2015, Maximillian Schrems/Data Protection Commissioner («Schrems»), C-362/14, ECLI:EU:C:2015:650, n. º 73.

([6]) Acórdão Schrems, n.º 74

([7]) Ver Comunicação da Comissão ao Parlamento Europeu e ao Conselho intitulada «Intercâmbio e proteção de dados pessoais num mundo globalizado», COM(2017) 7, de 10 de janeiro de 2017, secção 3.1, p. 6.

([8]) Acórdão Schrems, n.ºs 88 e 89.

([9]) Comité Europeu para a Proteção de Dados, documento de referência relativo à adequação, WP 254 rev. 01, disponível na seguinte ligação: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108.

([10]) 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 (JO L 207 de 1.8.2016, p. 1).

([11]) Acórdão Schrems II, n.º 185.

([12]) Acórdão Schrems II, n.º 197.

([13]) 28 CFR Part 302.

([14]) 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 Decisão do Comité Misto que incorpora o Regulamento (UE) 2016/679 no anexo XI do Acordo EEE foi adotada pelo Comité Misto do EEE em 6 de julho de 2018 e entrou em vigor em 20 de julho de 2018. Por conseguinte, o regulamento é abrangido pelo referido acordo. Para efeitos da decisão, as referências à UE e aos Estados-Membros da UE devem, pois, ser entendidas como abrangendo também os Estados do EEE.

(8) A presente decisão tem por efeito possibilitar as transferências de dados pessoais de responsáveis pelo tratamento e subcontratantes na União ([15]) para organizações certificadas nos EUA sem necessidade de obter qualquer outra autorização. A mesma não afeta a aplicação direta do Regulamento (UE) 2016/679 às referidas organizações que preencham as condições relativas ao âmbito de aplicação territorial do regulamento em apreço, previstas no seu artigo 3.º.

2. O QUADRO DE PRIVACIDADE DE DADOS UE-EUA

2.1. Âmbito de aplicação pessoal e material

2.1.1 *Organizações certificadas*

(9) O QPD UE-EUA baseia-se num sistema de certificação através do qual as organizações dos EUA se comprometem com um conjunto de princípios de privacidade — os princípios do Quadro de Privacidade dos Dados UE-EUA, incluindo os princípios suplementares (coletivamente, «os princípios») — emitidos pelo *Department of Commerce* (DoC) dos EUA e constantes do anexo II da presente decisão ([16]). Para ser elegível para certificação no âmbito do QPD UE-EUA, uma organização deve estar sujeita aos poderes de investigação e execução da *Federal Trade Commission* (FTC) ou do *Department of Transportation* (DOT) dos EUA ([17]). Os princípios devem ser aplicáveis imediatamente após a certificação. Tal como explicado mais circunstanciadamente nos considerandos 48 a 52, as organizações do QPD UE-EUA são obrigadas a proceder à renovação anual da certificação da sua adesão aos princípios ([18]).

2.1.2. *Definição de dados pessoais e conceitos de responsável pelo tratamento e «agente»*

(10) A proteção conferida no âmbito do QPD UE-EUA é aplicável a quaisquer dados pessoais transferidos da União para organizações localizadas nos EUA que tenham certificado a sua adesão aos princípios junto do DoC, com exceção dos dados recolhidos para efeitos de publicação, difusão ou outras formas de comunicação pública de material jornalístico e informação constante de material já publicado e arquivado ([19]). Por conseguinte, essas informações não podem ser transferidas com base no QPD UE-EUA.

(11) Os princípios definem os dados pessoais/informação pessoal da mesma forma que o Regulamento (UE) 2016/679, ou seja, «os dados que se referem a uma pessoa identificada ou identificável, que entrem no âmbito do RGPD e que, sendo provenientes da UE, sejam recebidos por entidades norte-americanas, independentemente da forma em que se encontrem registados» ([20]). Por conseguinte, também abrangem dados de investigação pseudonimizados (ou codificados com chave) (incluindo os casos em que a chave não é partilhada com a entidade norte-americana que recebe os dados) ([21]). Do mesmo modo, a noção de tratamento é definida como «qualquer operação ou conjunto de operações sobre dados pessoais, efetuadas com ou sem meios automatizados, 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» ([22]).

(12) O QPD UE-EUA é aplicável às organizações localizadas nos EUA consideradas como responsáveis pelo tratamento (ou seja, um cidadão ou organização que, de forma autónoma ou em conjunto com outros, determina as finalidades e os meios do tratamento de dados pessoais) ([23]) ou como subcontratantes (ou seja, agentes que atuam em nome de um responsável pelo tratamento) ([24]). Os subcontratantes norte-americanos devem ser contratualmente obrigados a agir apenas mediante instruções do responsável europeu pelo tratamento e ajudar este último a responder aos

([15]) A presente decisão não afeta os requisitos constantes do Regulamento (UE) 2016/679 aplicáveis às entidades (responsáveis pelo tratamento e subcontratantes) na União que transferem os dados, por exemplo, em matéria de limitação das finalidades, minimização dos dados, transparência e segurança dos dados [ver também o artigo 44.º do Regulamento (UE) 2016/679].

([16]) A este respeito, ver Schrems, n.º 81, em que o Tribunal de Justiça confirma que um sistema de autocertificação pode assegurar um nível de proteção adequado.

([17]) Anexo I, secção I.2. A FTC tem amplas competências em matéria de atividades comerciais, com algumas exceções, por exemplo, no que diz respeito a bancos, companhias aéreas, atividades de seguros e atividades de empresas públicas de telecomunicações (embora a decisão do Tribunal de Recurso dos EUA do Ninth Circuit, de 26 de fevereiro de 2018, no processo FTC v. AT&T tenha confirmado que a FTC tem jurisdição sobre as atividades privadas dessas entidades). Ver também o anexo IV, nota de rodapé 2. O DoT é competente para impor o cumprimento por parte das companhias aéreas e das agências de viagens (para o transporte aéreo), ver anexo V, secção A.

([18]) Anexo I, secção III.6.

([19]) Anexo I, secção III.2.

([20]) Anexo I, secção I.8.a.

([21]) Anexo I, secção III.14.g.

([22]) Anexo I, secção I.8.b.

([23]) Anexo I, secção I.8.c.

([24]) Ver, por exemplo, o anexo I, secção II.2.b, e secção II.3.b e 7.d, que esclarecem que os agentes atuam em nome de um responsável pelo tratamento, sujeitos às instruções deste último e ao abrigo de obrigações contratuais específicas.

pedidos dos cidadãos que exercem os seus direitos por força dos princípios ([25]). Além disso, no caso de subcontratação ulterior, um subcontratante deve celebrar um contrato com o subcontratante ulterior que assegure o mesmo nível de proteção previsto pelos princípios e tomar medidas para assegurar a sua aplicação adequada ([26]).

2.2. **Princípios do Quadro de Privacidade de Dados UE-EUA**

2.2.1. ***Limitação das finalidades e escolha***

(13) Os dados pessoais devem ser objeto de um tratamento lícito e leal. Devem ser recolhidos para uma finalidade específica e utilizados posteriormente apenas na medida em que essa utilização não seja incompatível com a finalidade do tratamento.

(14) No âmbito do QPD UE-EUA, esta utilização é assegurada através de diferentes princípios. Em primeiro lugar, no âmbito do *princípio de integridade dos dados e limitação das finalidades*, à semelhança do artigo 5.º, n.º 1, alínea b), do Regulamento (UE) 2016/679, uma organização não pode tratar dados pessoais de modo incompatível com a finalidade que motivou a recolha original ou que tenha sido autorizada, subsequentemente, pelo titular dos dados ([27]).

(15) Em segundo lugar, antes de utilizar os dados pessoais para uma nova finalidade (alterada) significativamente diferente, mas que ainda seja compatível com a finalidade original, ou para os divulgar a terceiros, a organização deve proporcionar aos titulares dos dados a oportunidade de se oporem (opção de não participação), de acordo com o *princípio de escolha* ([28]), através de um mecanismo claro, transparente e facilmente acessível. É importante salientar que este princípio não se substitui à proibição expressa dos tratamentos incompatíveis ([29]).

([25]) Anexo I, secção III.10.a. Ver igualmente as orientações elaboradas pelo DoC, em consulta com o Comité Europeu para a Proteção de Dados ao abrigo do Escudo de Privacidade, que esclarecem as obrigações dos subcontratantes norte-americanos que recebem dados pessoais da União ao abrigo do quadro. Uma vez que estas regras não foram alteradas, estas presentes orientações/perguntas frequentes continuam a ser pertinentes no âmbito do QPD UE-EUA (https://www.privacyshield.gov/article?id=Processing-FAQs).

([26]) Anexo I, secção II.3.b.

([27]) Anexo I, secção II.5.a. As finalidades compatíveis podem incluir atividades de auditoria, a prevenção da fraude ou outros objetivos coerentes com as expectativas de uma pessoa razoável, tendo em conta o contexto em que se inscreve a recolha (ver anexo I, nota de rodapé 6).

([28]) Anexo I, secção II.2.a. Esta circunstância não é aplicável quando uma organização fornece dados pessoais a um subcontratante que atua em seu nome e sob as suas instruções (anexo I, secção II.2.b). Dito isto, neste caso, a organização deve ter um contrato em vigor e assegurar o cumprimento do *princípio de responsabilização pela transferência ulterior*, tal como descrito mais circunstanciadamente no considerando 43. Além disso, o *princípio de escolha* (bem como o *princípio de aviso*) pode ser restringido quando os dados pessoais são tratados no contexto de auditorias jurídicas (no âmbito de uma potencial fusão ou aquisição) ou de auditorias, na medida em que tal se justifique, e pelo tempo necessário, para cumprir requisitos legais ou de interesse público, ou na medida em que tal se justifique, e pelo tempo necessário, em que a aplicação destes princípios seja prejudicial aos interesses legítimos da organização no contexto específico de auditorias jurídicas ou de auditorias (anexo I, secção III.4). O princípio suplementar 15 (anexo I, secção III.15.a e b) também prevê uma exceção ao princípio de escolha (bem como aos princípios de aviso e de responsabilização pela transferência ulterior) para os dados pessoais provenientes de fontes disponíveis ao público (salvo se o exportador de dados da UE indique que a informação está sujeita a restrições que exigem a aplicação desses princípios) ou para os dados pessoais recolhidos de registos abertos à consulta do público em geral (desde que não sejam combinados com informações de registos não disponíveis ao público e sejam respeitadas quaisquer condições de consulta). Do mesmo modo, o princípio suplementar 14 (anexo I, secção III.14.f) prevê uma exceção ao princípio de *escolha* (bem como aos princípios de *aviso* e de *responsabilização pela transferência ulterior*) para o tratamento de dados pessoais por uma empresa de dispositivos farmacêuticos ou médicos para atividades de controlo da segurança e da eficácia do produto, na medida em que a adesão aos princípios interfira com o cumprimento dos requisitos regulamentares.

([29]) Tal é aplicável a todas as transferências de dados efetuadas no âmbito do QPD UE-EUA, nomeadamente quando estas dizem respeito a dados recolhidos no contexto de uma relação laboral. Embora uma organização norte-americana certificada 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. Excecionalmente, uma organização pode utilizar dados pessoais para uma nova finalidade compatível sem respeitar os princípios de aviso e escolha, mas apenas na medida e durante o período necessários para evitar prejudicar a capacidade da organização para efetuar promoções, nomeações ou outras decisões semelhantes em matéria de emprego [ver anexo I, secção III.9.b., subalínea iv)]. A proibição feita à organização americana de aplicar sanções contra o assalariado que expressou a sua escolha, nomeadamente entravar a sua carreira profissional, garante que, apesar da relação de subordinação e de dependência inerente, não é exercida qualquer pressão sobre o assalariado, podendo este, por conseguinte, efetuar a sua escolha com total liberdade. Ver anexo I, secção III.9.b.(i).

2.2.2. ***Tratamento de categorias especiais de dados pessoais***

(16) Devem existir garantias específicas aplicáveis ao tratamento de «categorias especiais» de dados.

(17) Em conformidade com o *princípio de escolha*, aplicam-se garantias específicas ao tratamento de «informações sensíveis», ou seja, dados pessoais que especifiquem condições de saúde ou doenças, origem racial ou étnica, opiniões políticas, crenças religiosas ou filosóficas, pertença a sindicatos ou informações relativas à vida sexual do cidadão ou quaisquer outras informações recebidas de terceiros que sejam identificadas e tratadas por essa parte como sensíveis ([30]). Tal significa que quaisquer dados considerados sensíveis nos termos da legislação da União em matéria de proteção de dados (incluindo os dados relativos à orientação sexual, os dados genéticos e os dados biométricos) são tratados como sensíveis no âmbito do QPD UE-EUA pelas organizações certificadas.

(18) Regra geral, as organizações devem obter a autorização afirmativa expressa (ou seja, a opção de participação) dos cidadãos para utilizarem informações sensíveis para finalidades diferentes das que, inicialmente, motivaram a sua recolha ou da finalidade posteriormente autorizada pelos cidadãos (através do exercício da opção de participação) ou para a sua divulgação a terceiros ([31]).

(19) Esta autorização não tem de ser obtida em circunstâncias limitadas, semelhantes às exceções comparáveis previstas na legislação da União em matéria de proteção de dados, por exemplo, quando o tratamento de dados sensíveis é do interesse vital de uma pessoa, for necessário para a preparação de processos judiciais ou for necessário para prestar cuidados médicos ou elaborar um diagnóstico ([32]).

2.2.3. ***Exatidão, minimização e segurança dos dados***

(20) Os dados pessoais devem ser exatos e, se necessário, atualizados. Devem também ser adequados, pertinentes e não excessivos relativamente às finalidades para que são tratados e, em princípio, não devem ser conservados por mais tempo do que o necessário para as finalidades para que são tratados.

(21) No âmbito do *princípio de integridade dos dados e limitação das finalidades* ([33]), os dados pessoais devem limitar-se ao que é relevante para a finalidade do tratamento. Além disso, as organizações devem, na medida do necessário para as finalidades do tratamento, tomar providências razoáveis para assegurar que os dados pessoais são fiáveis para a utilização prevista, exatos, completos e atuais.

(22) Além disso, as informações pessoais só podem ser conservadas sob uma forma que permita identificar um cidadão ou o torne identificável (portanto, sob a forma de dados pessoais) ([34]) enquanto a sua utilização seja conforme à finalidade ou às finalidades para as quais foram inicialmente recolhidas ou posteriormente autorizadas, de acordo com o *princípio de escolha*. Esta obrigação não impede que as organizações continuem a tratar informações pessoais por períodos mais longos, mas apenas durante o tempo e na medida em que esse tratamento sirva razoavelmente para uma das finalidades específicas seguintes, semelhantes às exceções comparáveis previstas na legislação da União em matéria de proteção de dados: arquivamento no interesse público, jornalismo, literatura e arte, bem como investigação histórica e análise estatística ([35]). Quando os dados pessoais são conservados para uma destas finalidades, o seu tratamento está sujeito às garantias previstas nos princípios ([36]).

(23) Além disso, os dados pessoais devem ser tratados de uma forma que garanta a sua segurança, incluindo proteção contra tratamento não autorizado ou ilícito e contra perda, destruição ou danos acidentais. Para este fim, os responsáveis pelo tratamento e os subcontratantes devem tomar as medidas técnicas e organizativas adequadas para proteger os dados pessoais contra eventuais ameaças. Estas medidas devem ser avaliadas tendo em conta o estado da técnica, os custos conexos e a natureza, o âmbito, o contexto e as finalidades do tratamento, bem como os riscos para os direitos dos cidadãos.

([30]) Anexo I, secção II.2.c.
([31]) Anexo I, secção II.2.c.
([32]) Anexo I, secção III.1.
([33]) Anexo I, secção II.5.
([34]) Ver o anexo I, nota de rodapé 7, que esclarece que uma pessoa é considerada «identificável», desde que uma organização ou um terceiro possa razoavelmente identificá-la tendo em conta os meios de identificação que apresentem uma probabilidade razoável de serem utilizados (considerando, entre outros aspetos, os custos e o tempo necessário para a identificação e a tecnologia disponível à data do tratamento).
([35]) Anexo I, secção II.5.b.
([36]) *Ibid.*

(24) No âmbito do QPD UE-EUA, tal é assegurado pelo *princípio de segurança*, que exige, à semelhança do artigo 32.º do Regulamento (UE) 2016/679, a adoção de medidas de segurança razoáveis e adequadas, tendo em conta os riscos inerentes ao tratamento e a natureza dos dados ([37]).

2.2.4. ***Transparência***

(25) Os titulares dos dados devem ser informados sobre as principais características do tratamento dos respetivos dados pessoais.

(26) Tal é assegurado pelo *princípio de aviso* ([38]) que, à semelhança dos requisitos de transparência previstos no Regulamento (UE) 2016/679, exige que as organizações informem os titulares dos dados sobre, nomeadamente: i) a participação da organização no QPD, ii) o tipo de dados recolhidos, iii) a finalidade do tratamento, iv) o tipo ou a identidade de terceiros a quem os dados pessoais podem ser divulgados e as finalidades dessa divulgação, v) os seus direitos individuais, vi) a forma de contactar a organização, e vii) as vias de recurso disponíveis.

(27) Esta informação deve ser fornecida numa linguagem clara e visível, sempre que seja solicitado aos cidadãos que forneçam dados pessoais pela primeira vez ou logo que possível depois desse momento, mas em qualquer caso antes de os dados serem utilizados para uma finalidade substancialmente diferente (mas compatível) daquela para que foram recolhidos ou antes de serem divulgados a terceiros ([39]).

(28) Além disso, as organizações devem tornar públicas as suas políticas de privacidade que reflitam os princípios (ou, no caso dos dados relativos aos recursos humanos, disponibilizá-los imediatamente aos cidadãos em causa) e fornecer ligações para o sítio Web do *DoC* (com mais pormenores sobre a certificação, os direitos dos titulares dos dados e os mecanismos de recurso disponíveis), a lista do Quadro de Privacidade de Dados (lista do QPD) das organizações participantes e o sítio Web de um prestador de resolução alternativa de litígios adequado ([40]).

2.2.5. ***Direitos individuais***

(29) Os titulares dos dados devem ter determinados direitos que podem ser exercidos contra o responsável pelo tratamento ou subcontratante, nomeadamente o direito de acesso aos dados, o direito de oposição ao tratamento e o direito de retificação e apagamento dos dados.

(30) O *princípio de acesso* ([41]) do QPD UE-EUA confere aos cidadãos esses direitos. Em especial, os titulares dos dados têm o direito, sem necessidade de justificação, de obter junto de uma organização a confirmação de que está a tratar dados pessoais que lhes digam respeito, que os dados lhes sejam comunicados e de obter informações sobre a finalidade do tratamento, as categorias de dados pessoais que estão a ser tratados e os destinatários (categorias) a quem os dados são divulgados ([42]). As organizações são obrigadas a responder aos pedidos de acesso num prazo razoável ([43]). Uma

([37]) Anexo I, secção II.4.a. Além disso, no que diz respeito aos dados relativos aos recursos humanos, o QPD UE-EUA exige que os empregadores tenham em conta as opções dos trabalhadores em matéria de privacidade, restringindo o acesso aos dados pessoais, tornando determinados dados anónimos ou atribuindo códigos ou pseudónimos [anexo I, secção III.9.b.(iii)].

([38]) Anexo I, secção II.1.

([39]) Anexo I, secção II.1.b. O princípio suplementar 14 (anexo I, secção III.14.b e c) estabelece disposições específicas aplicáveis ao tratamento de dados pessoais no contexto da investigação no domínio da saúde e dos ensaios clínicos. Em especial, este princípio permite que as organizações tratem dados relativos a ensaios clínicos mesmo depois de um cidadão se ter retirado do ensaio, se tal tiver sido esclarecido no aviso fornecido quando o cidadão concordou em participar. Do mesmo modo, quando uma organização do QPD UE-EUA recebe dados pessoais para fins de investigação no domínio da saúde, só pode utilizá-los numa nova atividade de investigação de acordo com os princípios de *aviso* e de *escolha*. Neste caso, o aviso do cidadão deve, em princípio, fornecer informações sobre quaisquer futuras utilizações específicas dos dados (por exemplo, estudos conexos). Se não for possível incluir, desde o início, todas as futuras utilizações dos dados (porquanto novos conhecimentos ou desenvolvimentos médicos/investigação podem promover uma nova utilização para fins de investigação), deve ser incluída uma explicação de que os dados podem ser utilizados em futuras atividades de investigação médica e farmacêutica não previstas. Se essa utilização posterior não for coerente com as finalidades gerais de investigação para as quais os dados foram recolhidos (ou seja, se as novas finalidades forem substancialmente diferentes, mas ainda assim compatíveis com a finalidade original, ver considerandos 14-15), é necessário obter uma nova autorização (ou seja, *opt-in*). Ver, a título complementar, as restrições/exceções específicas ao princípio de *aviso* referidas na nota de rodapé 28.

([40]) Anexo I, secção III.6.d.

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

([42]) Anexo I, secção III.8.a. i)-ii).

([43]) Anexo I, secção III.8.i.

organização pode estabelecer limites razoáveis quanto ao número de vezes que podem ser aceites pedidos de acesso de um cidadão num determinado período e pode cobrar uma taxa que não seja excessiva, por exemplo, quando os pedidos são manifestamente excessivos, em especial devido ao seu caráter repetitivo ([44]).

(31) O direito de acesso só pode ser limitado em circunstâncias excecionais, semelhantes às previstas na legislação da União em matéria de proteção de dados, nomeadamente quando impliquem a violação dos direitos legítimos de terceiros, quando os encargos ou as despesas para facultar o acesso forem desproporcionados em relação aos riscos para a vida privada do cidadão nas circunstâncias do caso (embora os encargos e as despesas não sejam fatores de controlo para determinar se o acesso facultado é razoável), na medida em que a divulgação seja passível de interferir com a salvaguarda de interesses públicos igualmente importantes, em especial a segurança nacional, a segurança pública ou a defesa, se a informação contiver informações comerciais confidenciais, ou se a informação for tratada exclusivamente para fins de investigação ou estatísticos ([45]). 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 ([46]). Ao proceder a essa avaliação, a organização deve ter especialmente em conta os interesses do indivíduo ([47]). Sempre que for possível separar a informação de outros dados aos quais é aplicável uma limitação, a organização deve suprimir a informação protegida e divulgar a restante informação ([48]).

(32) Além disso, os titulares dos dados têm o direito de obter a retificação ou a alteração de dados inexatos, bem como a eliminação de dados que tenham sido tratados em violação dos princípios ([49]). Acresce que, conforme explicado no considerando 15, as pessoas têm o direito de se oporem ao tratamento dos seus dados para finalidades significativamente diferentes (mas compatíveis) que motivaram a recolha dos dados e à divulgação dos seus dados a terceiros. Quando os dados pessoais são utilizados para efeitos de comercialização direta, os cidadãos têm o direito geral de se oporem ao tratamento em qualquer momento ([50]).

(33) Os princípios não abordam, em específico, a questão das decisões que afetam o titular dos dados baseadas exclusivamente no tratamento automatizado dos dados pessoais. No entanto, no que se refere aos dados pessoais recolhidos na União, regra geral, qualquer decisão baseada num tratamento automatizado deve ser tomada pelo responsável pelo tratamento na União (que tem uma relação direta com o titular dos dados em causa), estando, por conseguinte, sujeita ao Regulamento (UE) 2016/679 ([51]). Tal inclui cenários de transferência em que o tratamento seja realizado por um operador comercial estrangeiro (por exemplo, EUA), que atua como agente (subcontratante) do responsável pelo tratamento na União (ou como subcontratante ulterior do subcontratante da União, o qual por sua vez recebeu os dados de um responsável pelo tratamento da União que os recolheu) que, nesta base, toma então a decisão.

(34) Este aspeto foi confirmado por um estudo encomendado pela Comissão em 2018 no contexto da segunda análise anual do funcionamento do Escudo de Proteção da Privacidade ([52]), que concluiu que, na altura, não existiam provas que sugerissem que as organizações aderentes ao Escudo de Proteção da Privacidade estavam, em geral, a tomar decisões automatizadas com base em dados pessoais transferidos no âmbito do Escudo de Proteção da Privacidade.

([44]) Anexo I, secção III.8.f. i)-ii) e g.
([45]) Anexo I, secção III.4. 8.b, c, e; 14.e, f and 15.d.
([46]) Anexo I, secção III.8.e.ii). A organização deve informar a pessoa em causa dos motivos da recusa/limitação e fornecer um ponto de contacto para quaisquer outras questões [secção III.8.a.(iii)].
([47]) Anexo I, secção III.8.a. ii)-iii).
([48]) Anexo I, secção III.8.a. i).
([49]) Anexo I, secção II.6 e secção III.8.a.(i).
([50]) Anexo I, secção III.8.12.
([51]) Em contrapartida, no caso excecional em que o operador de uma organização norte-americana tenha uma relação direta com titular dos dados da União, aquela resulta normalmente do facto de o operador ter visado essa pessoa na União através da oferta de bens ou serviços ou do controlo do seu comportamento. Neste cenário, o operador de uma organização norte-americana será, ele próprio, abrangido pelo âmbito de aplicação do Regulamento (UE) 2016/679 (artigo 3.º, n.º 2), tendo, portanto, de cumprir diretamente a legislação da União relativa à proteção de dados.
([52]) Subponto 4.1.5 do documento de trabalho dos serviços da Comissão [SWD(2018) 497 final]. O estudo centrou-se: i) na medida em que as organizações aderentes ao Escudo de Proteção da Privacidade nos EUA tomam decisões que afetam os cidadãos com base no tratamento automatizado dos dados pessoais transferidos de empresas na UE no âmbito do Escudo de Proteção da Privacidade; e ii) nas garantias para os cidadãos que a legislação federal dos EUA prevê para este tipo de situações e as condições de aplicação dessas garantias.

(35) Em todo o caso, nos 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, habitação e seguros), o direito dos EUA proporciona proteções específicas contra as decisões negativas ([53]). 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. No domínio do crédito ao consumo, a *Fair Credit Reporting Act* (FCRA) e a *Equal Credit Opportunity Act* (ECOA) contêm garantias que proporcionam aos consumidores alguma forma de direito a uma explicação e o direito de contestar a decisão. Estas leis são pertinentes num vasto leque de domínios, designadamente o crédito, o emprego, a habitação e os seguros. Além disso, determinadas leis relativas à antidiscriminação, como o título VII do *Civil Rights Act* e o *Fair Housing Act*, protegem os cidadãos em relação a modelos utilizados na tomada de decisões automatizadas suscetíveis de conduzir à discriminação com base em certas características e concedem aos cidadãos o direito de contestar essas decisões, nomeadamente as automatizadas. No que diz respeito aos dados de saúde, a *Health Insurance Portability and Accountability Act* (HIPAA) *Privacy Rule*cria determinados direitos semelhantes aos do Regulamento (UE) 2016/679 no que toca ao acesso aos dados de saúde de caráter pessoal. Além disso, as orientações das autoridades norte-americanas exigem que os prestadores de serviços médicos recebam informações que lhes permitam informar os cidadãos sobre os sistemas automatizados de tomada de decisões utilizados no setor médico ([54]).

(36) Por conseguinte, estas normas proporcionam proteções semelhantes às previstas na legislação da União em matéria de proteção de dados na situação improvável em que sejam tomadas decisões automatizadas pela própria organização do QPD UE-EUA.

2.2.6. ***Restrições relativas a transferências ulteriores***

(37) O nível de proteção conferido aos dados pessoais transferidos da União para as organizações nos Estados Unidos não pode ser prejudicado pela transferência subsequente desses dados para um destinatário nos Estados Unidos ou noutro país terceiro.

(38) No âmbito do princípio da responsabilização pela transferência ulterior ([55]), são aplicáveis regras especiais às transferências designadas como «ulteriores», ou seja, às transferências de dados pessoais de uma organização aderente ao QPD UE-EUA 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). Qualquer transferência ulterior só pode ter lugar: i) para finalidades limitadas e específicas, ii) com base num contrato entre a organização do QPD UE-EUA e o terceiro ([56]) (ou num acordo comparável no âmbito de um grupo de empresas ([57])), e iii) se esse contrato exigir unicamente que o terceiro assegure o mesmo nível de proteção que o garantido pelos princípios.

(39) Esta obrigação de proporcionar o mesmo nível de proteção que o garantido pelos princípios, em combinação com o *princípio de integridade dos dados e limitação das finalidades*, implica, nomeadamente, que terceiros só podem tratar as informações pessoais que lhes sejam transmitidas para finalidades que não sejam incompatíveis com as finalidades que motivaram a recolha ou que tenham sido autorizadas posteriormente pelo cidadão (de acordo com o *princípio de escolha*).

([53]) Ver, por exemplo, o *Equal Credit Opportunity Act* (15 U.S.C. 1691 e seg.), o *Fair Credit Reporting Act* (15 USC § 1681 e seg.) ou o *Fair Housing Act* (42 U.S.C. 3601 e seg.). Acresce que os Estados Unidos aderiram aos princípios da Organização de Cooperação e Desenvolvimento Económicos sobre Inteligência Artificial, que incluem, nomeadamente, princípios em matéria de transparência, capacidade de explicação, segurança e responsabilização.

([54]) Ver, por exemplo, as orientações disponíveis na página 2042-What personal health information do individuals have a right under HIPAA to access from their health care providers and health plans? | HHS.gov.

([55]) Ver anexo I, secção II.3, e o princípio suplementar «Contratos obrigatórios para transferências ulteriores» (anexo I, secção III.10).

([56]) Como exceção a este princípio geral, uma organização pode transferir ulteriormente dados pessoais de um pequeno número de trabalhadores sem celebrar um contrato com o destinatário para suprir necessidades operacionais ocasionais relacionadas com o emprego, por exemplo, a reserva de um voo ou de um quarto de hotel ou a cobertura de seguro. No entanto, também neste caso, a organização continua a ter de cumprir os princípios de *aviso* e de *escolha* (ver anexo I, secção III.9.e).

([57]) Ver igualmente o princípio suplementar «Contratos obrigatórios para as transferências posteriores» (anexo II, secção III.10.b). 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 certificada continuará a ser responsável pelo respeito do princípio, terá todo o interesse em utilizar instrumentos realmente eficazes na prática.

(40) O *princípio de responsabilização pela transferência ulterior* deve ser lido em conjugação com o *princípio de aviso* e, em caso de transferência posterior para um responsável pelo tratamento num país terceiro ([58]), com o *princípio da escolha*, segundo o qual os titulares de dados devem ser informados (entre outros) 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.

(41) 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 ulterior.

(42) 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, lhe cabe informar do facto a organização aderente ao QPD UE-EUA. Nesse caso, o tratamento pelo terceiro deve cessar ou devem ser tomadas outras medidas razoáveis e adequadas para corrigir a situação ([59]).

(43) Estão previstas proteções suplementares em caso de transferência posterior para um agente terceiro (um subcontratante). Nesse caso, a organização norte-americana deve assegurar que o agente atua apenas segundo as suas instruções e toma medidas razoáveis e adequadas i) para garantir que o agente 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 ([60]). O DoC pode solicitar à organização que forneça um resumo ou uma cópia representativa das disposições do contrato em matéria de privacidade ([61]). Se surgirem problemas de conformidade numa cadeia de (sub)contratação ulterior, a organização que atua na qualidade de responsável pelo tratamento dos dados pessoais é, em princípio, responsabilizada, tal como especificado no *princípio de recurso, aplicação e responsabilidade*, salvo se a organização provar que não é responsável pela situação conducente aos danos ([62]).

2.2.7. ***Responsabilização***

(44) De acordo com o princípio da responsabilização, as entidades responsáveis pelo tratamento de dados devem aplicar medidas técnicas e organizativas adequadas para cumprir as suas obrigações de proteção dos dados de forma eficaz e poder demonstrar esse cumprimento, em particular junto da autoridade de controlo competente.

(45) Quando uma organização tenha decidido, a título voluntário, certificar ([63]) no âmbito do QPD UE-EUA, a sua conformidade efetiva com os princípios é obrigatória e executória. No âmbito do *princípio de recurso, aplicação e responsabilidade* ([64]), as organizações do QPD UE-EUA devem prever mecanismos eficazes para assegurar a conformidade com os princípios. As organizações devem também tomar medidas para verificar ([65]) que as suas políticas 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 privacidade e que a conformidade é periodicamente reapreciada de forma objetiva, ou verificações de conformidade externas, cujos métodos podem incluir auditorias, verificações aleatórias ou a utilização de ferramentas tecnológicas.

([58]) Os titulares de dados não poderão opor-se quando os dados pessoais são transferidos para um terceiro que age na qualidade de agente para desempenhar tarefas por conta e segundo as instruções da organização norte-americana. Contudo, deve ter sido assinado um contrato entre o agente e a organização norte-americana, incumbindo a esta última garantir a proteção proporcionada pelos princípios, exercendo os seus poderes de instrução.

([59]) A situação é diferente consoante o terceiro seja um responsável pelo tratamento ou um subcontratante (agente). 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 aderente ao QPD UE-EUA - enquanto organização responsável pelo tratamento, atuando o agente sob as suas instruções - tomar essas medidas. Ver anexo I, secção II.3.

([60]) Anexo I, secção II.3.b.

([61]) *Ibid*.

([62]) Anexo I, secção II.7.d.

([63]) Ver igualmente o princípio suplementar «Autocertificação» (anexo I, seção III.6).

([64]) Ver igualmente o princípio suplementar «Resolução de litígios e aplicação» (anexo I, secção III.11.).

([65]) Ver igualmente o princípio suplementar «Verificação» (anexo I, seção III.7).

(46) Além disso, as organizações devem conservar registos sobre a aplicação das suas práticas no âmbito do QPD UE-EUA e disponibilizá-los, mediante pedido, a um organismo independente de resolução de litígios ou a uma autoridade responsável pela aplicação da lei competente no contexto de uma investigação ou de uma queixa por incumprimento ([66]).

2.3. **Administração, supervisão e execução**

(47) O DoC será responsável pela administração e controlo do QPD UE-EUA. O QPD UE-EUA prevê mecanismos de supervisão e de aplicação destinados a verificar e garantir que as organizações do QPD UE-EUA cumprem 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 III), pela FTC (anexo IV) e pelo *Department of Transportation* (anexo V).

2.3.1. ***Renovação da certificação***

(48) Para se certificarem no âmbito do QPD UE-EUA (ou para renovarem a certificação numa base anual), as organizações são obrigadas a declarar publicamente o seu compromisso em cumprir os princípios, disponibilizar as suas políticas de privacidade e aplicá-las na íntegra ([67]). No âmbito da sua declaração de renovação da certificação, as organizações têm de apresentar informações ao DoC sobre, entre outros elementos, o nome da organização relevante, uma descrição das finalidades para as quais a organização tratará os dados pessoais, os dados pessoais que serão abrangidos pela certificação, bem como o método de verificação escolhido, o mecanismo de recurso independente pertinente e o organismo oficial com competência para impor o cumprimento dos princípios ([68]).

(49) As organizações podem receber dados pessoais com base no QPD UE-EUA a contar da data em que são incluídas na lista do QPD pelo DoC. Para garantir a segurança jurídica e evitar «falsas alegações», as organizações que se certificam pela primeira vez não estão autorizadas a referir publicamente a sua adesão aos princípios antes de o DoC determinar a completude da declaração de certificação apresentada pela organização e de incluir a organização na lista do QPD ([69]). Para poder continuar a basear-se no QPD UE-EUA para receber dados pessoais da União, as organizações devem renovar anualmente a certificação da sua adesão ao quadro. Quando uma organização abandona o QPD UE-EUA por qualquer motivo, deve suprimir todas as declarações que sugiram que a organização continua a participar no quadro ([70]).

(50) Tal como refletido nos compromissos estabelecidos no anexo III, o DoC verifica se as organizações cumprem todos os requisitos de certificação e se adotaram uma política de privacidade (pública) que contenha as informações exigidas pelo princípio de aviso ([71]). Com base na experiência adquirida com o processo de renovação da certificação no âmbito do Escudo de Proteção da Privacidade, o DoC procederá a uma série de verificações, nomeadamente para verificar se as políticas de privacidade das organizações contêm uma ligação para o formulário correto para a apresentação de queixas no sítio Web do mecanismo de resolução de litígios pertinente e, quando várias entidades e filiais de uma organização constarem de uma declaração de certificação, se as políticas de privacidade de cada uma dessas entidades cumprem os requisitos de certificação e estão facilmente acessíveis aos titulares dos dados ([72]). Além disso, sempre que necessário, o DoC efetua verificações cruzadas com a FTC e o DOT para verificar se as organizações estão sujeitas ao organismo de supervisão indicado nos seus pedidos de renovação da certificação e colabora com os organismos de resolução alternativa de litígios para verificar se as organizações estão registadas no mecanismo de recurso independente constante da sua declaração de certificação ou de renovação da certificação ([73]).

([66]) Anexo I, secção III.7.
([67]) Anexo I, secção I.2.
([68]) Anexo I, secção III.6.b, e anexo III, secção «Verificar os requisitos de autocertificação».
([69]) Anexo I, nota de rodapé 12.
([70]) Anexo I, secção III.6.h.
([71]) Anexo I, secção III.6.a, e nota de rodapé 12, bem como o anexo III, secção «Verificar os requisitos de autocertificação».
([72]) Anexo III, secção «Verificar os requisitos de autocertificação».
([73]) Do mesmo modo, o DoC colabora com o terceiro que será o depositário dos fundos obtidos através de uma taxa para o painel das APD (ver considerando 73) para verificar se as organizações que escolhem as APD como o seu mecanismo de recurso independente pagaram a taxa relativa ao ano em causa. Ver anexo III, secção «Verificar os requisitos de autocertificação».

(51) O *Department of Commerce* informa as organizações de que, para concluírem a renovação da certificação, devem resolver todas as questões identificadas durante a sua análise. No caso de uma organização não responder dentro do prazo fixado pelo DoC (por exemplo, no que respeita à renovação da certificação, espera-se que o processo esteja concluído no prazo de 45 dias) ([74]) ou não concluir a sua certificação, a declaração será considerada como rejeitada. Nesse caso, quaisquer declarações falsas sobre a participação ou o cumprimento com o QPD UE-EUA podem ser objeto de medidas coercivas por parte da FTC ou do DOT ([75]).

(52) Para que o QPD 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 garantir essa transparência no «ponto de entrada», o DoC comprometeu-se a manter e a disponibilizar ao público a lista das organizações que certificaram a sua adesão aos princípios e que são abrangidas pelo âmbito de competência de, pelo menos, uma das autoridades responsáveis pela aplicação da lei referidas nos anexos IV e V da presente decisão ([76]). 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 QPD UE-EUA. Além disso, para garantir a transparência também no «ponto de saída», o DoC manterá e disponibilizará ao público um registo das organizações que foram suprimidas da lista, indicando, em cada caso, o motivo dessa supressão ([77]). Por último, fornecerá uma ligação para a página Web da FTC relativa ao QPD UE-EUA, em que figuram as medidas coercivas adotadas pela FTC no âmbito do quadro ([78]).

2.3.2. ***Controlo do cumprimento***

(53) O DoC fiscalizará continuamente o cumprimento efetivo dos princípios pelas organizações do QPD UE-EUA através de diferentes mecanismos ([79]). Em especial, efetuará «controlos esporádicos» a organizações selecionadas aleatoriamente, bem como controlos esporádicos *ad hoc* a organizações específicas quando forem identificados potenciais problemas de cumprimento (por exemplo, comunicados ao *Department of Commerce* por terceiros), a fim de verificar se: i) existem pontos de contacto para tratar queixas e pedidos dos titulares dos dados e se lhes dão resposta; ii) a política de privacidade da organização está facilmente acessível, tanto no seu sítio Web como através de uma ligação no sítio Web do *Department of Commerce*; iii) a política de privacidade da organização continua a cumprir os requisitos de certificação; e iv) o mecanismo independente de resolução de litígios escolhido pela organização está disponível para proceder ao tratamento das queixas ([80]).

(54) Se existirem provas credíveis de que uma organização não cumpre os compromissos assumidos no âmbito do QPD UE-EUA (em especial, se o DoC receber queixas ou se a organização não responder satisfatoriamente aos inquéritos do DoC), o DoC exigirá que a organização preencha e apresente um questionário pormenorizado ([81]). Uma organização que não responda de forma satisfatória e atempada ao questionário será remetida para a autoridade competente (a FTC ou o DOT) para a aplicação de eventuais medidas coercivas ([82]). No âmbito das suas atividades de verificação de conformidade no contexto do Escudo de Proteção da Privacidade, o DoC efetuou verificações aleatórias regulares a que se refere o considerando 53 e controlou continuamente os relatórios públicos, o que lhe

([74]) Anexo III, nota de rodapé 2.
([75]) Ver anexo III, secção «Verificar os requisitos de autocertificação».
([76]) As informações sobre a gestão da lista do QPD constam do anexo III (ver a introdução da rubrica «Administração e supervisão do programa do Quadro de Privacidade de Dados pelo *Department of Commerce*») e do anexo I (secção I.3, secção I.4, secção III.6.d, e secção III.11.g).
([77]) Anexo III, ver a introdução da rubrica «Administração e supervisão do programa do Quadro de Privacidade de Dados pelo *Department of Commerce*».
([78]) Ver anexo III, secção «Adaptar o sítio Web do Quadro de Privacidade de Dados a públicos específicos».
([79]) Ver anexo III, secção «Realizar verificações de conformidade oficiosas sistemáticas e avaliações do programa do Quadro de Privacidade de Dados».
([80]) No âmbito das suas atividades de controlo, o DoC pode utilizar diferentes ferramentas, incluindo a verificação de ligações obsoletas para políticas de privacidade ou controlar ativamente notícias relacionadas com relatórios que forneçam provas credíveis de não conformidade.
([81]) Ver anexo III, secção «Realizar verificações de conformidade oficiosas sistemáticas e avaliações do programa do Quadro de Privacidade de Dados».
([82]) Ver anexo III, secção «Realizar verificações de conformidade oficiosas sistemáticas e avaliações do programa do Quadro de Privacidade de Dados».

permitiu identificar, abordar e resolver problemas de cumprimento ([83]). As organizações que de maneira persistente não cumpram os princípios devem ser suprimidas da lista do QPD e devem devolver ou eliminar os dados pessoais recebidos ao abrigo do quadro ([84]).

(55) Noutros casos de supressão, como a retirada voluntária ou a não renovação da certificação, a organização deve apagar ou devolver os dados, ou pode conservá-los, desde que confirme anualmente ao DoC o seu compromisso de continuar a aplicar os princípios ou garanta 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 pertinentes aprovadas pela Comissão) ([85]). Neste caso, as organizações devem ainda identificar um ponto de contacto na organização para o esclarecimento de todas as questões relacionadas com o QPD UE-EUA.

2.3.3. ***Identificação e resolução de falsas alegações de adesão***

(56) O DoC controlará quaisquer falsas alegações de participação no QPD UE-EUA ou a utilização indevida da marca de certificação do QPD UE-EUA, tanto oficiosamente como com base em queixas (por exemplo, recebidas das APD) ([86]). Em especial, o DoC verificará continuamente se as organizações que: i) deixem de participar no QPD UE-EUA, ii) não efetuam a renovação da certificação anual (ou seja, iniciaram, mas não concluíram o processo de renovação da certificação anual em tempo útil ou não chegaram a iniciar o processo de renovação da certificação anual), iii) sejam excluídas como participantes, em particular devido a «incumprimento persistente», ou iv) não efetuam a certificação inicial (ou seja, iniciaram, mas não concluíram o processo de renovação da certificação inicial em tempo útil), suprimem qualquer política de privacidade publicada pertinente das referências ao QPD UE-EUA que sugira que a organização participa ativamente no quadro ([87]). O DoC também efetuará pesquisas na Internet para identificar referências ao QPD UE-EUA nas políticas de privacidade das organizações, designadamente para identificar falsas alegações de organizações que nunca participaram no QPD UE-EUA ([88]).

(57) Se o DoC verificar que as referências ao QPD UE-EUA não foram suprimidas ou são utilizadas indevidamente, informará a organização sobre um eventual recurso junto da FTC/ do DOT ([89]). Se uma organização não responder de forma satisfatória, o DoC submeterá a questão para a agência competente para a aplicação de potenciais medidas coercivas ([90]). Quaisquer declarações falsas prestadas ao público em geral por uma organização relativas à sua adesão aos princípios, sob a forma de declarações ou práticas enganosas, estão sujeitas a medidas coercivas por parte da FTC, do DOT ou de outras autoridades norte-americanas responsáveis pela aplicação da lei. As falsas declarações prestadas ao *Department of Commerce* são passíveis de impugnação judicial nos termos do *False Statements Act* (legislação sobre falsas declarações — 18 USC § 1001).

([83]) Durante a segunda reapreciação anual do Escudo de Proteção da Privacidade, o DoC informou que tinha efetuado controlos esporádicos em cem organizações e enviado questionários de conformidade em 21 casos (após os quais foram retificados os problemas detetados). Ver o documento de trabalho dos serviços da Comissão [SWD(2018) 497 final, p. 9]. Do mesmo modo, o *Department of Commerce* comunicou que, durante a terceira reapreciação anual do Escudo de Proteção da Privacidade, ao proceder ao controlo de relatórios públicos, havia detetado três incidentes, tendo iniciado a prática de efetuar, mensalmente, controlo esporádicos em 30 empresas, o que resultou em questionários de conformidade em 28 % dos casos (após os quais os problemas detetados foram imediatamente corrigidos ou, em três casos, resolvidos após uma carta de advertência). Ver o documento de trabalho dos serviços da Comissão [SWD(2019) 495 final, p. 8].

([84]) Anexo I, secção III.11.g. Um incumprimento persistente ocorre, em especial, quando uma organização se recusa a cumprir uma decisão final de qualquer autoridade de autorregulamentação em matéria de privacidade, autoridade independente de resolução de litígios ou autoridade responsável pela aplicação da lei.

([85]) Anexo I, secção III.6.f.

([86]) Ver anexo III, secção sobre «Procura e Resolução de falsas declarações de adesão».

([87]) *Ibid.*

([88]) *Ibid.*

([89]) *Ibid.*

([90]) No âmbito do Escudo de Proteção da Privacidade, o DoC comunicou, durante a terceira análise anual do quadro, ter identificado 669 casos de falsas alegações de participação (entre outubro de 2018 e outubro de 2019), a maioria das quais foram resolvidas após a carta de advertência do DoC, tendo 143 casos sido remetidos para a FTC (ver considerando 62 *infra*). Ver o documento de trabalho dos serviços da Comissão [SWD(2019) 495 final, p. 10].

2.3.4. ***Aplicação***

(58) A fim de assegurar que seja garantido, na prática, um nível adequado de proteção dos dados, deve ser criada uma autoridade de controlo independente incumbida de supervisionar a aplicação das normas em matéria de proteção de dados e de as fazer cumprir.

(59) As organizações do QPD UE-EUA devem estar sujeitas à jurisdição das autoridades competentes dos EUA, ou seja, a FTC e o DOT, que têm os poderes de investigação e execução necessários para assegurar o cumprimento efetivo dos princípios ([91]).

(60) A FTC é uma autoridade independente constituída por cinco comissários, nomeados pelo presidente com o conselho e consentimento do Senado ([92]). Os comissários são nomeados por um período de sete anos e só podem ser destituídos pelo presidente por ineficiência, negligência do dever ou prevaricação. A FTC não pode ter mais de três comissários do mesmo partido político e os comissários não podem, durante a sua nomeação, dedicar-se a qualquer outro negócio, vocação ou emprego.

(61) A FTC pode investigar o cumprimento dos princípios, bem como falsas alegações de adesão aos princípios ou de participação no QPD UE-EUA por parte de organizações que já não constem da lista do QPD ou que nunca foram certificadas ([93]). A FTC pode assegurar o cumprimento dos princípios através de decisões proferidas por tribunais administrativos ou federais (incluindo «injunções» obtidas por meio de acordos) ([94]) relativas a injunções preliminares ou permanentes ou outras reparações e controlará sistematicamente o cumprimento dessas decisões ([95]). Quando as organizações não cumpram essas decisões, a FTC pode solicitar sanções de caráter civil e outras reparações, designadamente por quaisquer danos provocados pela conduta ilegal. Todas as injunções dirigidas a uma organização aderente ao QPD UE-EUA devem incluir disposições de comunicação pela própria organização ([96]), devendo estas organizações publicar todas as secções pertinentes relacionadas com o QPD UE-EUA dos relatórios de conformidade ou avaliação apresentados à FTC. Por último, a FTC manterá uma lista em linha das organizações objeto de decisões judiciais ou da FTC em processos relativos ao QPD UE-EUA ([97]).

(62) No que diz respeito ao Escudo de Proteção da Privacidade, a FTC aplicou medidas coercivas a cerca de 22 processos, tanto no que toca a violações de requisitos específicos do quadro (por exemplo, a omissão de confirmação ao DoC de que a organização continuava a aplicar as proteções do Escudo de Proteção da Privacidade depois de ter saído do quadro, a não verificação, através de uma autoavaliação ou de uma verificação de conformidade externa, de que a organização cumpria o quadro) ([98]) como a falsas alegações de participação no quadro (por exemplo, por organizações que não cumpriram as fases necessárias para obter a certificação ou que deixaram caducar a sua certificação, mas que continuaram falsamente a referir a sua participação no quadro) ([99]). Estas medidas coercivas resultaram, nomeadamente, da utilização proativa de intimações administrativas para obter materiais de determinados participantes no Escudo de Proteção da Privacidade, a fim de verificar a existência de violações significativas das obrigações do Escudo de Proteção da Privacidade ([100]).

([91]) Uma organização que aderiu ao QPD UE-EUA tem de declarar publicamente o seu compromisso em cumprir os princípios, divulgar as suas políticas de proteção da privacidade em conformidade com estes princípios e aplicá-los na íntegra. O incumprimento pode ser sujeito a medidas coercivas nos termos da secção 5 da FTC Act que proíbe atos desleais e enganosos no comércio ou que o afetem (15 U.S.C. § 45) e 49 U.S.C. § 41712, que proíbe uma transportadora ou a uma agência de viagens de praticar práticas desleais ou enganosas no transporte aéreo ou na venda de passagens aéreas.

([92]) 15 U.S.C. § 41.

([93]) ANEXO IV

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

([95]) Ver anexo IV, secção «Obtenção e acompanhamento de decisões».

([96]) 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.

([97]) Anexo IV, secção «Obtenção e acompanhamento de decisões».

([98]) Documento de trabalho dos serviços da Comissão [SWD(2019) 495 final, p. 11].

([99]) Ver os processos constantes do sítio Web da FTC, disponíveis em: https://www.ftc.gov/business-guidance/privacy-security/privacy-shield. Ver também os documentos de trabalho dos serviços da Comissão SWD(2017) 344 final, p. 17, SWD(2018) 497 final, p. 12, e SWD(2019) 495 final, p. 11.

([100]) Ver, por exemplo, as observações do presidente Joseph Simons na segunda análise anual do Escudo de Proteção da Privacidade (ftc.gov).

(63) De um modo mais geral, nos últimos anos, a FTC tomou medidas coercivas numa série de casos relativos ao cumprimento de requisitos específicos em matéria de proteção de dados também previstos ao abrigo do QPD UE-EUA, por exemplo, no que diz respeito aos princípios da limitação da finalidade e da conservação dos dados ([101]), da minimização dos dados ([102]), da segurança ([103]) e da exatidão dos dados ([104]).

(64) 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. Os funcionários do DoT têm como primeiro objetivo chegar a um acordo e, se tal não for possível, podem instaurar um processo de execução que implica uma audição de provas perante um juiz de direito administrativo do DoT, que tem competência para emitir decisões para fazer cessar e proibir as práticas desleais ([105]). Os juízes de direito administrativo beneficiam de várias proteções nos termos da *Administrative Procedure Act* (APA) por forma a garantir a sua independência e imparcialidade. Por exemplo, só podem ser destituídos por justa causa, os processos são-lhes atribuídos alternadamente, não podem exercer funções incompatíveis com as suas funções e responsabilidades enquanto juízes de direito administrativo, não estão sujeitos à supervisão da equipa de investigação da autoridade para a qual trabalham (neste caso, o DOT) e devem exercer a sua função executiva/jurisdicional de modo imparcial ([106]). O DoT comprometeu-se a controlar os despachos de execução e a assegurar que as decisões resultantes de processos relativos ao QPD UE-EUA estão disponíveis no seu sítio Web ([107]).

2.4. **Reparação**

(65) A fim de assegurar uma proteção adequada e, nomeadamente, o exercício dos direitos individuais, o titular dos dados deve dispor de vias de recurso administrativas e judiciais eficazes.

(66) O QPD UE-EUA determina, através do *princípio* de *recurso, aplicação e responsabilidade*, que as organizações criem vias de recurso em caso de incumprimento, e que, deste modo, os titulares de dados da União, possam apresentar queixas por incumprimento por parte de organizações do QPD UE-EUA e obtenham a resolução dessas queixas, se necessário mediante uma decisão de reparação efetiva ([108]). No quadro da sua certificação, as organizações devem satisfazer os requisitos deste princípio, 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 cidadãos ([109]).

([101]) Ver, por exemplo, o despacho da FTC no processo Drizly, LLC., entre outros, que exige que a empresa 1) destrua quaisquer dados pessoais recolhidos que não sejam necessários para fornecer produtos ou prestar serviços aos consumidores, 2) abster-se de recolher ou armazenar informações pessoais, a menos que tal seja necessário para fins específicos descritos num calendário que fixe os períodos de conservação.

([102]) Ver, por exemplo, o despacho da FTC no processo CafePress (24 de março de 2022), que impõe, nomeadamente, a minimização da quantidade de dados recolhidos.

([103]) Ver, por exemplo, as medidas coercivas da FTC nos processos Drizzly, LLC e CafePress, onde foi imposta às empresas em causa a implementação de um programa de segurança específico ou medidas de segurança específicas. Além disso, no que respeita às violações de dados, ver também o despacho da FTC de 27 de janeiro de 2023, no processo Chegg, o acordo alcançado com a Equifax em 2019 (https://www.ftc.gov/news-events/news/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related-2017-data-breach).

([104]) Ver, por exemplo, o processo RealPage, Inc (16 de outubro de 2018), em que a FTC tomou medidas coercivas ao abrigo da FCRA contra uma empresa de triagem de arrendatários que forneceu a proprietários e empresas de gestão de imóveis dados sobre indivíduos, com base em informações provenientes de historiais de arrendamento, registos públicos (incluindo antecedentes criminais e de despejo) e informações de crédito, que foram utilizadas como fator para determinar a elegibilidade para o arrendamento de habitação. A FTC constatou que a empresa não tomou medidas razoáveis para garantir a exatidão das informações que forneceu com base no seu instrumento de autodecisão.

([105]) Ver anexo V, secção «Práticas de execução».

([106]) Ver 5 U.S.C. §§ 3105, 7521(a), 554(d) e 556(b)(3).

([107]) Ver anexo V, secção «Controlo e publicação de despachos de execução relativos a violações do QPD UE-EUA».

([108]) Anexo I, secção II.7.

([109]) Anexo I, secção III.11.

(67) As organizações podem escolher mecanismos de recurso independentes na União ou nos Estados Unidos, Conforme explicado mais circunstanciadamente no considerando 73, tal inclui a possibilidade de se comprometerem, a título voluntário, em cooperar com as APD da UE. Sempre que as organizações tratem dados relativos a recursos humanos, esse compromisso de cooperação com as APD da UE é obrigatório. Outras alternativas incluem um organismo independente de resolução alternativa de litígios ou 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.

(68) Por conseguinte, o QPD UE-EUA fornece aos titulares de dados um certo número de possibilidades para fazerem valer os seus direitos, apresentarem queixas em caso de incumprimento pelas organizações do QPD UE-EUA e de essas queixas serem resolvidas, se necessário mediante uma decisão de reparação efetiva. Os titulares de dados podem apresentar uma queixa diretamente a uma organização, um organismo independente de resolução de litígios designado pela organização, às APD nacionais, ao *Department of Commerce* ou à FTC. Nos casos em que essas queixas não foram resolvidas por um desses mecanismos de recurso ou de aplicação, os cidadãos têm igualmente o direito de invocar uma arbitragem vinculativa (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 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.

(69) Em primeiro lugar, os titulares de dados da União podem impugnar os casos de incumprimento dos princípios através de contactos diretos com as organizações do QPD UE-EUA ([110]). 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 os cidadãos 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), bem como sobre o organismo independente de resolução de litígios designado (ver considerando 70). Após a receção de uma queixa individual, independentemente de ser apresentada diretamente pelo interessado ou através do DoC na sequência de um reenvio por uma APD, a organização deve fornecer uma resposta ao titular de dados da União no prazo de 45 dias ([111]). Do mesmo modo, as organizações devem responder rapidamente às questões e a outros pedidos de informações relativos à sua adesão aos princípios que lhes são dirigidos pelo DoC ou por uma APD ([112]) (quando a organização se tenha comprometido a cooperar com a APD).

(70) Em segundo lugar, os titulares de dados podem também apresentar uma queixa diretamente a um organismo independente de resolução de litígios (quer nos Estados Unidos ou na União) designado pela organização para investigar e resolver queixas individuais (salvo se evidentemente infundadas ou abusivas) e para proporcionar uma via de recurso adequada a título gratuito para o titular dos dados ([113]). As reparações e sanções aplicadas por esse 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 ([114]). Os organismos independentes para a resolução de litígios designados por uma organização são obrigados a incluir nos seus sítios Web públicos informações pertinentes sobre o QPD UE-EUA e os serviços que prestam neste âmbito ([115]). Todos os anos, devem publicar um relatório anual com estatísticas agregadas relativas a estes serviços ([116]).

([110]) Anexo I, secção III.11.d. i).

([111]) Anexo I, secção III.11.d. i).

([112]) 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» (anexo I, secção III.5).

([113]) Anexo I, secção III.11.d.

([114]) Anexo I, secção II.7 e secção III.11.e.

([115]) Anexo I, secção III.11.d.(ii).

([116]) O relatório anual deve incluir o seguinte: 1) o número total de queixas relacionadas com o QPD UE-EUA 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.

(71) No âmbito dos respetivos procedimentos de verificação da conformidade, o DoC pode verificar se as organizações do QPD UE-EUA estão efetivamente registadas junto dos mecanismos de recurso independentes nos quais alegam estar registadas ([117]). 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 QPD UE-EUA. O DoC colaborará com os mecanismos de recurso independentes para verificar se incluem nos seus sítios Web informações relativas aos princípios e aos serviços que prestam no âmbito do QPD UE-EUA e se publicam relatórios anuais ([118]).

(72) Nos casos em que a organização não cumpra a decisão de um organismo de autorregulação ou de resolução de litígios, este deve notificar o incumprimento ao DoC e à FTC (ou a outra entidade norte-americana com competência para investigar o incumprimento por parte da organização), ou a um tribunal competente ([119]). 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 concluir que, frequentemente, uma organização não cumpre os princípios, tal pode ser considerado como um incumprimento sistemático o que implica que o DoC, após dar à organização que não cumpriu um pré-aviso de 30 dias e uma oportunidade para responder, procederá à supressão da referida organização da lista ([120]). Se, uma vez suprimida da lista, a organização continuar a alegar a sua certificação no âmbito do QPD UE-EUA, o DoC submeterá a questão à FTC ou outro órgão ou agente da autoridade ([121]).

(73) Em terceiro lugar, as pessoas singulares podem também apresentar as suas reclamações a uma APD nacional na União, que pode utilizar os seus poderes de investigação e reparação ao abrigo do Regulamento (UE) 2016/679. 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 ([122]). 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 ([123]). Em caso de não seguimento do aconselhamento prestado pela APD, a APD remeterá esses casos para o DoC (que pode retirar organizações da lista de QPD UE-EUA) ou, com vista a eventuais medidas coercivas, para a FTC ou o DoT (a não cooperação com as APD ou a violação dos princípios é passível de recurso ao abrigo da legislação dos EUA) ([124]).

(74) Para facilitar a cooperação para um tratamento eficaz das queixas, tanto o DoC como a FTC criaram um ponto de contacto específico responsável pela ligação direta com as APD ([125]). Esses pontos de contacto assistem nas consultas das APD relativas ao cumprimento dos princípios por parte de uma organização.

(75) O aconselhamento prestado pelas APD ([126]) é emitido após ter sido dada a ambas as partes envolvidas uma oportunidade razoável para apresentar observações e fornecer todas as informações sobre as provas que considerem necessárias. O painel pode prestar aconselhamento o mais rapidamente possível, dentro dos limites processuais permitidos, regra geral, nos 60 dias seguintes à receção da queixa ([127]). Se uma organização não aplicar o conselho da APD no prazo de 25 dias, sem apresentar uma razão válida para o atraso, o painel pode comunicar a sua intenção de submeter 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, esta situação poderá conduzir a

([117]) Anexo I, secção «Verificar os requisitos de autocertificação».
([118]) Ver anexo III, secção «Facilitar a cooperação com os organismos de resolução alternativa de litígios que prestam serviços relacionados com os princípios». Ver também o anexo I, secção III.11.d.(ii)-(iii).
([119]) Ver anexo I, secção III.11.e.
([120]) Ver anexo I, secção III.11.g., em especial os pontos ii) e iii).
([121]) Ver anexo III, secção sobre «Procura e Resolução de falsas declarações de participação».
([122]) Anexo I, secção II.7.b.
([123]) Anexo I, secção III.5.
([124]) Anexo I, secção III.5.c.(ii).
([125]) Anexo III (ver a secção «Facilitar a cooperação com as APD») e anexo IV (ver as secções «Atribuição de prioridade às transmissões de queixas e investigações» e «Cooperação em matéria de execução com as APD da UE»).
([126]) 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.
([127]) Anexo I, secção III.5.c. i).

medidas de execução com base na secção 5 da FTC Act (ou lei semelhante) ([128]). 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 QPD.

(76) 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 da UE.

(77) Os cidadãos 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 para o *Department of Commerce* ou para a FTC. Para facilitar e reforçar a cooperação em questões relacionadas com queixas individuais e com o incumprimento por parte das organizações aderentes ao QPD UE-EUA, o DoC criará um ponto de contacto específico que servirá de ponto de ligação com as APD e assisti-las-à nas investigações sobre o cumprimento dos princípios por parte de uma organização ([129]). Do mesmo modo, a FTC comprometeu-se a criar um ponto de contacto específico ([130]).

(78) Em quarto lugar, o DoC comprometeu-se a receber, verificar e envidar os melhores esforços para resolver queixas sobre o incumprimento dos princípios por parte de uma organização ([131]). Para esse efeito, o DoCprevê procedimentos especiais para que as APD reenviem queixas a um ponto de contacto dedicado, procedam ao seu rastreio e acompanhem as organizações a fim de facilitar a resolução ([132]). Com o intuito de acelerar o tratamento de queixas individuais, o ponto de contacto estabelece um contacto direto com a respetiva APD sobre questões de conformidade e, em especial, mantém-na atualizada sobre o estado das queixas num prazo máximo de 90 dias após a apresentação da queixa ([133]). Tal permite que os titulares de dados apresentem queixas de incumprimento imputadas a organizações do QPD UE-EUA diretamente à sua APD nacional e que estas sejam transmitidas ao *Department of Commerce* enquanto organização norte-americana que administra o QPD UE-EUA.

(79) Se, com base nas suas verificações sistemáticas, queixas ou quaisquer outras informações, o DoC concluir que uma organização não cumpriu de forma persistente os princípios, deve proceder à supressão da referida organização da lista do QPD ([134]). 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, deve ser considerada um incumprimento persistente ([135]).

(80) Em quinto lugar, uma organização do QPD UE-EUA deve estar sujeita à competência das autoridades norte-americanas, em especial da FTC ([136]), que tenham os poderes de investigação e execução necessários para assegurar o cumprimento efetivo dos princípios. A FTC dá prioridade às queixas de incumprimento dos princípios apresentadas por organismos independentes de resolução de litígios ou de autorregulação, pelo DoC 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 ([137]). 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, pode aceitar queixas diretamente dos cidadãos e proceder a investigações no âmbito do QPD UE-EUA por iniciativa própria, nomeadamente como parte da sua investigação em maior escala sobre questões relacionadas com a privacidade.

([128]) Anexo I, secção III.5.c.(ii).
([129]) Ver anexo III, secção «Facilitar a cooperação com as APD».
([130]) Ver anexo IV, secções «Atribuição de prioridade às transmissões de queixas e investigações» e «Cooperação em matéria de execução com as APD da UE».
([131]) Anexo III, ver, por exemplo, a secção «Facilitar a cooperação com as APD».
([132]) Anexo I, secção II.7, e anexo III, secção «Facilitar a cooperação com as APD».
([133]) *Ibid*.
([134]) Anexo I, secção III.11.g.
([135]) Anexo I, secção III.11.g.
([136]) Uma organização aderente ao QPD UE-EUA 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 pode ser sujeito a medidas coercivas nos termos da secção 5 da FTC Act, que proíbe atos desleais e enganosos no comércio ou que afetem o comércio.
([137]) Ver também os compromissos semelhantes assumidos pelo DOT, anexo V.

(81) 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 União pode invocar arbitragem vinculativa pelo Comité do Quadro de Privacidade de Dados UE-EUA (Comité do QPD UE-EUA) ([138]). As organizações devem informar os cidadãos sobre a possibilidade de invocar a arbitragem vinculativa e são obrigadas a responder quando os cidadãos por ela optem, devendo informar a organização em causa ([139]).

(82) Este Comité do QPD UE-EUA é constituído por um grupo de, pelo menos, dez árbitros que são designados pelo *Department of Commerce* e pela Comissão com base na sua independência e integridade, bem como na sua experiência na legislação dos EUA em matéria de privacidade e na legislação da União em matéria de proteção de dados. Para cada litígio, as partes selecionam a partir deste grupo um conjunto de um ou três ([140]) árbitros.

(83) O *Department of Commerce* escolheu o *International Centre for Dispute Resolution* (ICDR), a divisão internacional da *American Arbitration Association* (AAA), para administrar as arbitragens. Os procedimentos perante o Comité do QPD UE-EUA reger-se-ão por um conjunto de regras de arbitragem acordadas e por um código de conduta aplicável aos árbitros nomeados. O sítio Web do ICDR-AAA fornece informações claras e concisas aos cidadãos sobre o mecanismo de arbitragem e o procedimento para apresentar um pedido de arbitragem.

(84) As regras de arbitragem acordadas entre o *Department of Commerce* e a Comissão complementam o QPD UE-EUA, que contém várias características que melhoram a acessibilidade deste mecanismo para os titulares dos dados da União: 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 deve ser fornecida sem custos para o titular dos dados; iii) embora a língua utilizada na arbitragem seja, regra geral, o inglês, a interpretação na audiência arbitral e a tradução podem, em princípio ser fornecidas mediante pedido fundamentado e sem custos para o titular dos dados; iv) por último, embora cada parte tenha de suportar os honorários do próprio advogado, se for representada por um advogado perante o comité, o DoC criará um fundo alimentado por contribuições anuais das organizações aderentes ao QPD UE-EUA, destinadas a cobrir os custos elegíveis do procedimento arbitral até aos montantes máximos a determinar pelas autoridades dos EUA em consulta com a Comissão ([141]).

(85) O Comité do QPD UE-EUA tem competência para aplicar as «medidas equitativas, específicas do titular dos dados e não pecuniárias» ([142]) necessárias para corrigir o incumprimento dos princípios. Embora o comité tome em consideração outras reparações já obtidas através de outros mecanismos do QPD UE-EUA ao proferir a sua decisão, os cidadãos podem recorrer à arbitragem se considerarem que estas outras reparações são insuficientes. Tal permite que os titulares de dados da União invoquem a arbitragem em todos os casos nos quais a ação ou inação de organizações do QPD UE-EUA, mecanismos de recurso independentes ou as autoridades competentes dos EUA (por exemplo, a FTC), não tenha resolvido as suas queixas de forma satisfatória. Não é possível invocar a arbitragem se uma APD tiver autoridade jurídica para resolver a queixa em questão no que se refere à organização do QPD UE-EUA, nomeadamente nos casos em que esta 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. Os cidadãos podem solicitar a execução da decisão de arbitragem aos 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 de uma organização.

([138]) Ver anexo I do anexo I, «Modelo de arbitragem».
([139]) Ver anexo I, secção II.1.a.(xi) e secção II.7.c.
([140]) O número de árbitros no comité deve ser acordado entre as partes.
([141]) Anexo I do anexo I, secção G.6.
([142]) Os cidadãos não podem requerer uma indemnização por perdas e danos na arbitragem, mas a invocação de arbitragem não exclui a opção de solicitar uma essa indemnização nos tribunais comuns dos EUA.

(86) Em sétimo lugar, quando uma organização não cumpre o seu compromisso de respeitar os princípios e a política de privacidade publicada, a legislação dos EUA prevê vias de recurso judicial adicionais, nomeadamente a possibilidade de obter uma indemnização por danos. Por exemplo, os cidadãos podem, em determinadas condições, obter reparação judicial (incluindo indemnização por danos) nos termos da legislação estatal em matéria de defesa do consumidor em processos relativos a declarações fraudulentas, atos ou práticas desleais ou enganosas ([143]) e nos termos do direito civil (em especial, no âmbito dos delitos de ingerência na vida privada ([144]), apropriação de nome ou imagem ([145]) e divulgação pública de factos privados ([146])).

(87) Em conjunto, as várias vias de recurso acima descritas garantem que cada reclamação relativa ao incumprimento do QPD UE-EUA por parte de organizações certificadas será efetivamente tratada e corrigida.

3. ACESSO E UTILIZAÇÃO DE DADOS PESSOAIS TRANSFERIDOS DA UNIÃO EUROPEIA POR AUTORIDADES PÚBLICAS NORTE-AMERICANAS

(88) A Comissão avaliou igualmente as limitações e garantias, incluindo a supervisão e os mecanismos individuais de recurso previstos pelo direito dos EUA, no tocante à recolha e utilização subsequente pelas autoridades públicas norte-americanas de dados pessoais transferidos para responsáveis pelo tratamento e subcontratantes nos EUA, para fins de interesse público, designadamente para efeitos de aplicação do direito penal e de segurança nacional («acesso governamental») ([147]). Ao avaliar se as condições em que o governo acede aos dados transferidos para os Estados Unidos nos termos da presente decisão cumprem o teste de «equivalência essencial» em conformidade com o previsto pelo artigo 45.º, n.º 1, do Regulamento (UE) 2016/679, conforme interpretado pelo Tribunal de Justiça, à luz da Carta dos Direitos Fundamentais, a Comissão teve em conta os critérios apresentados *infra*.

(89) Em especial, qualquer restrição ao direito de proteção de dados pessoais deve ser prevista por lei, o que implica que a própria base jurídica que permite a interferência nesse direito deve definir o alcance da restrição no exercício do direito em causa ([148]). Além disso, para satisfazer o requisito da proporcionalidade, segundo o qual as derrogações à proteção de dados pessoais e as suas restrições devem ocorrer na estrita medida do necessário numa sociedade democrática para responder a objetivos específicos de interesse geral equivalentes aos reconhecidos pela União, esta base jurídica deve estabelecer regras claras e precisas que regulem o alcance e o âmbito de aplicação das medidas em causa e imponham requisitos mínimos para que os cidadãos cujos dados foram transferidos disponham de garantias suficientes que permitam proteger eficazmente os seus dados pessoais contra os riscos de abuso ([149]). Além disso,

([143]) Ver, por exemplo, as leis estatais relativas à defesa do consumidor na Califórnia [*Cal. Civ. Code* §§ 1750-1785 (*West*) *Consumers Legal Remedies Act*], Distrito de Colúmbia (*D.C. Code* §§ 28-3901), Florida (Fla. Stat. §§ 501.201 - 501.213, Deceptive and Unfair Trade Practices Act); Illinois (815 Ill. Comp. Stat. 505/1 - 505/12, Consumer Fraud and Deceptive Business Practices Act); Pennsylvania (73 Pa. Stat. Ann. §§ 201-1 - 201-9.3 (West) Unfair Trade Practices and Consumer Protection Law).

([144]) Ou seja, no caso de uma ingerência intencional na vida privada ou nos interesses privados de um cidadão, de uma forma que seja altamente ofensiva para uma pessoa razoável [*Restatement (2nd) of Torts*, § 652(b)].

([145]) Geralmente, este delito é aplicável em caso de apropriação e utilização do nome ou imagem de um cidadão para publicitar uma empresa ou um produto ou para qualquer outro fim comercial semelhante [ver *Restatement (2nd) of Torts*, § 652C].

([146]) Ou seja, quando é tornada pública informação sobre a vida privada de um cidadão, numa circunstância que seja altamente ofensiva para uma pessoa razoável, e não sendo essa informação do interesse legítimo do público [*Restatement (2nd) of Torts*, § 652D].

([147]) Isto é igualmente pertinente à luz da secção I.5 do anexo I. Nos termos dessa secção e também do RGPD, o cumprimento de requisitos e direitos em matéria de proteção de dados que fazem parte dos princípios de privacidade pode ser sujeito a limitações. No entanto, tais limitações não são absolutas, podendo ser invocadas apenas em determinadas condições, por exemplo, na medida do necessário para dar cumprimento a uma decisão judicial ou satisfazer requisitos de interesse público, de aplicação da lei ou de segurança nacional. Neste contexto, e por razões de clareza, a presente secção remete igualmente para as condições estabelecidas no EO 14086, que são avaliadas, nomeadamente, nos considerandos 127 a 141.

([148]) Ver acórdão do Tribunal de Justiça de 16 de julho de 2020, Facebook Ireland e Schrems («Schrems II»), C-311/18, ECLI:EU:C:2020:559, n.os 174 a 175, e a jurisprudência referida Ver também, no que diz respeito ao acesso das autoridades públicas dos Estados-Membros, o Acórdão do Tribunal de Justiça de 6 de outubro de 2020, Privacy International, C-623/17, ECLI:EU:C:2020:790, n.º 65, e o acórdão do Tribunal de Justiça de 6 de outubro de 2020, La Quadrature du Net e o., processos apensos C-511/18, C-512/18 e C-520/18, ECLI:EU:C:2020:791, n.º 175.

([149]) Ver acórdão do Tribunal de Justiça de 16 de julho de 2020, Facebook Ireland e Schrems («Schrems II»), C-311/18, ECLI:EU:C:2020:559, n.os 176 e 181, bem como a jurisprudência referida. Ver também, no que diz respeito ao acesso das autoridades públicas dos Estados-Membros, o Acórdão do Tribunal de Justiça de 6 de outubro de 2020, Privacy International, C-623/17, ECLI:EU:C:2020:790, n.º 68, e o Acórdão do Tribunal de Justiça de 6 de outubro de 2020, La Quadrature du Net e outros, C-511/18, C-512/18 e C-520/18, ECLI:EU:C:2020:791, n.º 132.

estas regras e garantias devem ser juridicamente vinculativas e poder ser aplicadas pelos cidadãos ([150]). Em particular, os titulares de dados devem dispor da possibilidade de recorrer a medidas jurídicas corretivas eficazes num tribunal independente e imparcial, para ter acesso a dados pessoais que lhes digam respeito ou para obter a retificação ou a supressão desses dados ([151]).

3.1. **Acesso e utilização pelas autoridades públicas norte-americanas para efeitos de aplicação do direito penal**

(90) No que diz respeito à ingerência nos dados pessoais transferidos no âmbito do QPD UE-EUA para efeitos de aplicação do direito penal, a legislação dos Estados Unidos impõe uma série de limitações ao acesso e à utilização de dados pessoais e prevê mecanismos de supervisão e recurso em conformidade com os requisitos referidos no considerando 89 da presente decisão. Os pontos seguintes descrevem as condições nas quais esse acesso pode ser efetuado e as garantias aplicáveis à utilização desses poderes. A este respeito, o Governo dos EUA [por intermédio do *Department of Justice* (DOJ)] também forneceu garantias sobre as limitações e garantias aplicáveis (anexo VI da presente decisão).

3.1.1. ***Bases jurídicas, limitações e garantias***

3.1.1.1 *Limitações e garantias no que respeita à recolha de dados pessoais para efeitos de aplicação do direito penal*

(91) Os procuradores federais e os agentes federais de investigação podem aceder, no contexto de diferentes procedimentos explicados mais circunstanciadamente nos considerandos 90 a 99, aos dados pessoais tratados por organizações norte-americanas certificadas e transferidos da União com base no QPD UE-EUA. Estes procedimentos aplicam-se da mesma forma quando a informação é obtida de qualquer organização norte-americana, independentemente da nacionalidade ou do local de residência dos titulares dos dados ([152]).

(92) Em primeiro lugar, a pedido de um agente federal responsável pela aplicação da lei ou de um advogado do governo, um juiz pode emitir um mandado de busca ou apreensão (incluindo de informações eletronicamente armazenadas) ([153]). Esse mandado só pode ser emitido se existir uma «causa provável» ([154]) de que os «objetos apreensíveis» (provas de um crime, objetos detidos ilegalmente ou bens concebidos ou destinados a serem utilizados ou usados para cometer um crime) são suscetíveis de ser encontrados no local especificado no mandado. O mandado deve indicar os bens ou os objetos a apreender e designar o juiz ao qual o mandado deve ser devolvido. Um cidadão sujeito a uma busca ou cujos bens sejam objeto de busca pode apresentar um pedido de supressão das

([150]) Ver acórdão do Tribunal de Justiça de 16 de julho de 2020, Facebook Ireland e Schrems («Schrems II»), C-311/18, ECLI:EU:C:2020:559, n.os 181 a 182.

([151]) Ver o Acórdão do Tribunal de Justiça de 16 de julho de 2020, Data Protection Commissioner («Schrems I»), C-311/18, ECLI:EU:C:2020:559, n.º 95, e o Acórdão do Tribunal de Justiça de 6 de outubro de 2015, Maximillian Schrems («Schrems II»), C-362/14, ECLI:EU:C:2015:650, n.º 194. A esse respeito, o TJUE salientou que a observância do artigo 47.º da Carta dos Direitos Fundamentais, que garante o direito à ação por um tribunal independente e imparcial, «faz parte do nível de proteção exigido na União [e] deve ser constatada pela Comissão antes de adotar uma decisão de adequação ao abrigo do artigo 45.º, n.º 1, do Regulamento (UE) 2016/679» (Schrems II, n.º 186).

([152]) Ver anexo VI. Ver, por exemplo, no que diz respeito à *Wiretap Act*, à *Stored Communications Act* e à *Pen Register Act* (leis referidas mais circunstanciadamente nos considerandos 92 a 98), Suzlon Energy Ltd/Microsoft Corp, 671 F.3d 726, 729 (9th Cir. 2011).

([153]) *Federal Rules of Criminal Procedure*, 41. Num acórdão de 2018, o Supremo Tribunal confirmou ser igualmente necessário um mandado de busca ou uma exceção relativa a um mandado de busca para as autoridades responsáveis pela aplicação da lei terem acesso às informações históricas de localização das células telefónicas que proporcionam uma visão geral dos movimentos de um utilizador e para que o utilizador possa ter uma expectativa razoável de privacidade no que diz respeito a essas informações [Timothy Ivory Carpenter/Estados Unidos da América, n.os 16 a 402, 585 U.S. (2018)]. Consequentemente, esses dados não podem, em geral, ser obtidos de uma empresa de telemóveis com base numa decisão judicial assente em motivos razoáveis para considerar que as informações são pertinentes e significativas para uma investigação penal em curso, mas exige a demonstração da existência de uma causa provável quando é utilizado um mandado.

([154]) De acordo com o Supremo Tribunal, por «causa provável» entende-se uma norma «prática e não técnica» que se baseia em «considerações factuais e práticas da vida quotidiana, com base nas quais os homens razoáveis e prudentes [...] agem» [Ilinóis/Gates, 462 U.S. 213, 232 (1983)]. No que respeita aos mandados de busca, existe uma causa provável quando há uma probabilidade razoável de que uma busca resulte na descoberta de provas de um crime (id.).

provas obtidas ou derivadas de uma busca ilegal, caso essas provas sejam apresentadas contra esse cidadão durante um processo penal ([155]). Quando um detentor dos dados (por exemplo, uma empresa) for obrigado a divulgar dados no âmbito de um mandado, pode contestar o requisito de divulgação por ser excessivamente oneroso ([156]).

(93) Em segundo lugar, no contexto de investigações de determinados crimes graves ([157]), geralmente a pedido de um procurador federal, um júri (um ramo de investigação do tribunal reunido por um juiz ou magistrado) pode emitir uma intimação para exigir que um cidadão apresente ou disponibilize documentação empresarial, informações eletronicamente armazenadas ou outros elementos tangíveis. Além disso, várias leis 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 ([158]). Em ambos os casos, as informações devem ser pertinentes para a investigação e a intimação não pode ser pouco razoável, ou seja, demasiado abrangente, opressiva ou onerosa (e pode ser contestada pelo destinatário da intimação com base nesses motivos) ([159]).

(94) Aplicam-se condições muito semelhantes às intimações administrativas emitidas para obter acesso a dados detidos por empresas nos EUA para fins civis ou regulamentares («interesse público»). A autoridade das agências com responsabilidades civis e regulamentares para emitir tais intimações administrativas deve ser estabelecida por lei. O recurso a uma intimação administrativa está sujeito a um «teste de razoabilidade», que exige que a investigação seja conduzida com um objetivo legítimo, que as informações solicitadas no âmbito da intimação sejam relevantes para esse efeito, que a agência não disponha já das informações que procura obter com a intimação e que tenham sido seguidas as diligências administrativas necessárias para a emitir ([160]). A jurisprudência do Supremo Tribunal também clarificou a necessidade de equilibrar a importância do interesse público nas informações solicitadas com a importância dos interesses pessoais e organizacionais em matéria de privacidade ([161]). Embora a utilização de uma intimação administrativa não esteja sujeita a aprovação judicial prévia, fica sujeita a controlo judicial em caso de contestação pelo destinatário pelos motivos acima referidos, ou se o organismo emissor pretender executar a intimação em tribunal ([162]). Para além destas limitações gerais, podem decorrer requisitos específicos (mais rigorosos) de leis específicas ([163]).

([155]) Ver *Mapp v. Ohio*, 367 U.S. 643 (1961).

([156]) Ver *In re Application of United States*, 610 F.2d 1148, 1157 (3d Cir.1979) (que determina que «o processo equitativo exige uma audiência sobre a questão da onerosidade antes de obrigar uma empresa telefónica a prestar» assistência com um mandado de busca) e *In re Application of United States*, 616 F.2d 1122 (9th Cir. 1980).

([157]) A Quinta Emenda da Constituição dos EUA exige que o júri deduza acusação relativamente a qualquer «crime capital ou de outro modo infame». O júri é constituído por 16 a 23 membros e determina se existe uma causa provável para considerar que foi cometido um crime. Para chegar a esta conclusão, os júris têm poderes de investigação que lhes permitem emitir intimações.

([158]) Ver anexo VI.

([159]) *Federal Rules of Criminal Procedure*, 17.

([160]) *United States v. Powell*, 379 U.S. 48 (1964)

([161]) *Oklahoma Press Publishing Co. v. Walling*, 327 U.S. 186 (1946).

([162]) O Supremo Tribunal clarificou que, em caso de contestação de uma intimação administrativa, um tribunal deve ponderar se 1) a investigação tem uma finalidade legalmente autorizada, 2) a competência por decretar a intimação administrativa em questão está sob o controlo do Congresso, e (3) os documentos solicitados são pertinentes para a investigação. O Tribunal notou igualmente que o pedido de uma intimação administrativa deve ser «razoável», isto é, especificar os documentos que são solicitados de forma adequada, mas não excessiva, para os efeitos da investigação pertinente e ser pormenorizados quanto à descrição do local onde devem ser feitas as buscas e das pessoas ou objetos a apreender.

([163]) Por exemplo, a lei relativa ao direito à privacidade financeira confere a uma autoridade governamental o poder de obter registos financeiros detidos por uma instituição financeira nos termos de uma intimação administrativa apenas se 1) existirem motivos para crer que os registos solicitados são pertinentes para uma investigação judicial legítima e 2) tiver sido fornecida ao cliente uma cópia da intimação ou convocação, juntamente com uma notificação que indique com razoável especificidade a natureza da investigação (12 U.S.C. § 3405). Outro exemplo é a *Fair Credit Reporting Act*, que proíbe as agências de informação dos consumidores de divulgarem relatórios de consumidores em resposta a pedidos de intimação administrativa (e apenas lhes permite responder a pedidos de intimação de um júri ou a decisões judiciais, 15 U.S.C. § 1681 e seg.). No que toca ao acesso a informações sobre comunicações, aplicam-se as exigências específicas da *Stored Communications Act*, nomeadamente no que diz respeito à possibilidade de recorrer a intimações administrativas (ver considerandos 96-97 para uma análise pormenorizada).

(95) Em terceiro lugar, várias bases jurídicas permitem às autoridades responsáveis pela aplicação do direito penal obter acesso a dados de comunicações. Um tribunal pode proferir uma decisão que autorize a recolha, em tempo real, de informações, não relativas ao conteúdo, sobre marcação, encaminhamento, endereçamento e sinalização de um número de telefone ou de um endereço de correio eletrónico (através da utilização de um dispositivo de registo de chamadas telefónicas e comunicações eletrónicas), se considerar que a autoridade certificou que as informações suscetíveis de serem obtidas são pertinentes para uma investigação criminal em curso ([164]). A decisão deve, entre outros elementos, especificar a identidade, se conhecida, do suspeito, os atributos das comunicações às quais é aplicável a decisão e a declaração da infração a que se referem as informações a recolher. A utilização de um dispositivo de registo de chamadas telefónicas e comunicações eletrónicas pode ser autorizada por um período máximo de 60 dias, que só pode ser prorrogado mediante uma nova decisão judicial.

(96) Além disso, o acesso, para fins de aplicação do direito penal, às informações sobre assinantes, aos dados de tráfego e ao conteúdo armazenado de comunicações detidos por prestadores de serviços de Internet, companhias telefónicas e outros prestadores de serviços pode ser obtido com base na *Stored Communications Act* ([165]). Para obter o conteúdo armazenado de comunicações eletrónicas as autoridades responsáveis pela aplicação do direito penal devem, em princípio, obter um mandado de um juiz com base numa causa provável para considerar que a conta em questão contém provas de um crime ([166]). 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 podem usar uma intimação. Para a restante informação armazenada não relativa ao conteúdo, como mensagens de endereço eletrónico sem assunto, uma autoridade responsável pela aplicação do direito penal deve obter uma decisão judicial, que é emitida se o juiz achar que existem motivos razoáveis para considerar que as informações solicitadas são pertinentes e significativas para uma investigação penal em curso.

(97) Os prestadores que recebam pedidos nos termos da *Stored Communications Act* podem notificar, a título voluntário, um cliente ou um assinante cujas informações sejam solicitadas, salvo quando a autoridade responsável pela aplicação do direito penal competente obtenha uma decisão cautelar que proíba essa notificação ([167]). Essa decisão cautelar é uma decisão judicial que exige que um prestador de serviços de comunicações eletrónicas ou de serviços de computação à distância a quem é dirigido um mandado, uma intimação ou uma decisão judicial não notifique qualquer outro cidadão da existência do mandado, da intimação ou da decisão judicial, durante o tempo que o tribunal considerar adequado. As decisões cautelares só são emitidas se o tribunal considerar que há razões para crer que a notificação pode prejudicar gravemente uma investigação ou adiar um julgamento de modo indevido, por exemplo, porque pode pôr em perigo a vida ou a segurança física de um cidadão, conduzir à fuga à justiça, intimidar potenciais testemunhas, etc. Um memorando do *Deputy Attorney General* (vinculativo para todos os advogados e agentes do DoJ) exige que os procuradores formulem uma decisão pormenorizada relativa à necessidade de uma decisão cautelar e que apresentem uma justificação ao tribunal sobre a forma como os critérios legais para a obtenção de uma decisão cautelar são cumpridos no processo específico ([168]). O memorando exige também que os pedidos de decisões cautelares não podem, em geral, adiar a notificação por mais de um ano. Nos casos em que, em circunstâncias excecionais, possam ser necessárias decisões cautelares de duração mais longa, essas decisões só podem ser solicitadas com o acordo escrito de um supervisor designado pelo *Attorney General* dos EUA ou pelo *Assistant Attorney General* competente. Além disso, um procurador deve, aquando do encerramento de uma investigação, avaliar imediatamente se existe uma base para manter efetivas quaisquer decisões cautelares e, se tal não for o caso, suspender a decisão cautelar e assegurar que o prestador de serviços é notificado do facto ([169]).

([164]) 18 U.S.C. § 3123.

([165]) 18 U.S.C. §§ 2701-2713.

([166]) 18 U.S.C. §§ 2701(a)-(b)(1)(A). Se o assinante ou o cliente em causa for notificado (antecipadamente ou, em determinadas circunstâncias, através de uma notificação tardia), as informações relativas ao conteúdo armazenadas durante mais de 180 dias também podem ser obtidas com base numa intimação administrativa ou numa intimação emitida pelo júri [18 U.S.C. §§ 2701(b)(1)(B)] ou numa decisão judicial (se existirem motivos razoáveis para considerar que as informações são pertinentes e significativas para uma investigação penal em curso [18 U.S.C. §§ 2701(d)]. No entanto, de acordo com uma decisão de um tribunal de recurso federal, os investigadores do governo obtêm mandados de busca geralmente de juízes para recolher o conteúdo de comunicações privadas ou dados armazenados de um prestador de serviços de comunicações comerciais. *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010).

([167]) 18 U.S.C. § 2705 (b).

([168]) Ver o memorando emitido pelo *Deputy Attorney General* Rod Rosenstein em 19 de outubro de 2017 sobre uma política mais restritiva em matéria de pedidos de decisões cautelares (ou de não divulgação), disponível em: https://www.justice.gov/criminal-ccips/page/file/1005791/download.

([169]) Memorando emitido pela *Deputy Attorney General* Lisa Moncao em 27 de maio de 2022 sobre uma política suplementar relativa aos pedidos de decisões cautelares nos termos do 18 U.S.C. § 2705(b).

(98) As autoridades responsáveis pela aplicação do direito penal podem também intercetar comunicações por cabo, orais ou eletrónicas em tempo real com base numa decisão judicial em que um juiz considere, nomeadamente, que existe uma causa provável para considerar que a escuta ou interceção eletrónica produzirá provas de um crime federal ou da localização de um fugitivo que foge à justiça ([170]).

(99) O DoJ fornece outras proteções no âmbito de várias políticas e orientações, incluindo as orientações do *Attorney General* sobre as operações nacionais do FBI (AGG-DOM), que, entre outros aspetos, exigem que o Federal Bureau of Investigation utilize os métodos de investigação menos intrusivos possíveis, tendo em conta o efeito na privacidade e nas liberdades cívicas ([171]).

(100) Segundo as declarações apresentadas pelo governo dos EUA, são aplicáveis as mesmas proteções ou mais elevadas descritas anteriormente às investigações das autoridades com funções coercivas a nível estadual (no que se refere às investigações levadas a cabo no âmbito das leis estaduais) ([172]). Em especial, disposições constitucionais, bem como regulamentos e jurisprudência estaduais, reafirmam as proteções acima referidas contra buscas e apreensões não razoáveis, ao exigir a emissão de um mandado de busca ([173]). À semelhança das proteções concedidas a nível federal, os mandados de busca só podem ser emitidos mediante a demonstração de uma causa provável e devem descrever o local a ser revistado e a pessoa ou coisa a apreender ([174]).

([170]) 18 U.S.C. §§ 2510-2522.

([171]) *Guidelines for Domestic Federal Bureau of Investigation (FBI) Operations*do *Attorney General* (setembro de 2008), disponíveis em: http://www.justice.gov/archive/opa/docs/guidelines.pdf. As regras e políticas adicionais que prescrevem limitações às atividades de investigação dos procuradores federais encontram-se estabelecidas no *United States Attorneys' Manual* disponível em http://www.justice.gov/usam/united-states-attorneys-manual. Para se afastar destas orientações, deve ser obtida a aprovação prévia do diretor do FBI, do diretor-adjunto ou do diretor-adjunto executivo designado pelo diretor, salvo se essa aprovação não puder ser obtida devido ao caráter imediato ou à gravidade de uma ameaça à segurança de cidadãos ou bens ou à segurança nacional (caso em que o diretor ou outra pessoa autorizada tem de ser notificada logo que possível). Se as orientações não forem respeitadas, o FBI deve notificar o DOJ, que, por sua vez, informa o *Attorney General* e o *Deputy Attorney General*.

([172]) Anexo VI, nota de rodapé 2. Ver também, por exemplo, *Arnold v. City of Cleveland*, 67 Ohio St.3d 35, 616 N.E.2d 163, 169 (1993) («Nos domínios dos direitos individuais e das liberdades cívicas, a Constituição dos Estados Unidos, quando aplicável aos Estados, estabelece um nível de proteção mínimo que deve ser respeitado nas decisões dos tribunais estatais»); *Cooper v. California*, 386 U.S. 58, 62, 87 S.Ct. 788, 17 L.Ed.2d 730 (1967) («A nossa deliberação, evidentemente, não afeta o poder do Estado de impor buscas e apreensões normas mais rigorosas do que as exigidas pela Constituição Federal se optar por fazê-lo.»); *Petersen v. City of Mesa*, 63 P.3d 309, 312 (Ariz. Ct. App. 2003) («Embora a Constituição do Estado de Arizona possa impor normas mais rigorosas em matéria de buscas e apreensões do que as previstas na Constituição federal, os tribunais do Arizona não podem garantir uma proteção inferior à garantida pela Quarta Emenda»).

([173]) A maioria dos Estados reproduziu as proteções da Quarta Emenda nas respetivas Constituições. Ver Alabama Const. art. I, § 5; Alaska Const. art. I, § 14; 1; Arkansas Const. art. II, § 15; California Const. art. I, § 13; Colorado Const. art. II, § 7; Conneticut Const. art. I, § 7; Delaware Const. art. I, § 6; Flórida. Const. art. I, § 12; Georgia Const. art. I, § I, para. XIII; Hawai Const. art. I, § 7; Idaho Const. art. I, § 17; Illinois Const. art. I, § 6; Indiana Const. art. I, § 11; Iowa Const. art. I, § 8; Kansas Const. Bill of Rights, § 15; Kentucky Const. § 10; Louisiana Const. art. I, § 5; Maine Const. art. I, § 5; Massachusets Const. Decl. of Rights art. 14; Michigan Const. art. I, § 11; Minnesota Const. art. I, § 10; Mississippi Const. art. III, § 23; Missouri Const. art. I, § 15; Montana Const. art. II, § 11; Nebraska Const. art. I, § 7; Nevad Const. art. I, § 18; New Hampshire Const. pt. 1, art. 19; N.J. Const. art. II, § 7; New Mexico Const. art. II, § 10; New York Const. art. I, § 12; North Dakota Const. art. I, § 8; Ohio Const. art. I, § 14; Oklahoma Const. art. II, § 30; Oregon Const. art. I, § 9; Pennsylvania Const. art. I, § 8; Rhode Island Const. art. I, § 6; South Carolina Const. art. I, § 10; South Dakota Const. art. VI, § 11; Tennessee Const. art. I, § 7; Texas Const. art. I, § 9; Utah Const. art. I, § 14; Vermont Const. ch. I, art. 11; West Virginia Const. art. III, § 6; Wisconsin Const. art. I, § 11; Wyoming Const. art. I, § 4. Outros Estados (por exemplo, Maryland, Carolina do Norte e Virgínia) consagraram nas respetivas constituições uma linguagem específica relativa aos mandados que foram interpretados judicialmente para proporcionar uma proteção semelhante ou superior à conferida pela Quarta Emenda (ver Maryland. Decl. of Rts. art. 26; North Carolina Const. art. I, § 20; Virginia Const. art. I, § 10, e jurisprudência relevante, e.g. *Hamel v. State*, 943 A.2d 686, 701 (Md. Ct. Spec. App. 2008; *State v. Johnson*, 861 S.E.2d 474, 483 (N.C. 2021) e *Lowe v. Commonwealth*, 337 S.E.2d 273, 274 (Va. 1985)). Por último, os Estados de Arizona e Washington têm disposições constitucionais que protegem a privacidade de um modo mais geral (Arizona Const. art. 2.º, § 8; Washington Const. art. I, § 7), que foram interpretadas pelos tribunais como proporcionando maior proteção do que a conferida pela Quarta Emenda (ver, por exemplo, *State v. Bolt*, 689 P.2d 519, 523 (Ariz. 1984), *State v. Ault*, 759 P.2d 1320, 1324 (Ariz. 1988), *State v. Myrick*, 102 Wn.2d 506, 511, 688 P.2d 151, 155 (1984) , *State v. Young*, 123 Wn.2d 173, 178, 867 P.2d 593, 598 (1994)).

([174]) Ver, por exemplo, California Penal Code § 1524,3(b); Rule 3.6-3.13 Alabama Rules of Criminal Procedure; Section 10.79.035; Revised Code of Washington; Section 19.2-59 of Chapter 5, Title 19.2 Criminal Procedure, Code of Virginia.

3.1.1.2 *Utilização adicional das informações recolhidas*

(101) No que se refere à utilização subsequente de dados recolhidos pelas autoridades federais responsáveis pela aplicação do direito penal, diferentes leis, orientações e normas impõem garantias específicas. Com exceção dos instrumentos específicos aplicáveis às atividades do FBI (AGG-DOM e *FBI Domestic Investigations and Operations Guide*), os requisitos descritos na presente secção aplicam-se geralmente à utilização posterior de dados por qualquer autoridade federal, incluindo os dados acedidos para fins civis ou regulamentares. Aqui se incluem os requisitos decorrentes das notas/regulamentos do *Office of Management and Budget*, da *Federal Information Security Management Modernization Act*, da *E-Government Act* e da *Federal Records Act*.

(102) De acordo com a autoridade prevista pela *Clinger-Cohen Act* (P.L. 104-106, secção E) e pela *Computer Security Act* de 1987 (P.L. 100-235), o *Office of Management and Budget* (OMB) emitiu a Circular n.º A-130 para estabelecer orientações gerais vinculativas aplicáveis a todas as agências federais (incluindo as autoridades responsáveis pela aplicação da lei) quando estas lidam com informações pessoais identificáveis ([175]). Em especial, a circular exige que todas as agências federais «limitem a criação, a recolha, a utilização, o tratamento, o armazenamento, a manutenção, a disseminação e a divulgação de informações pessoais identificáveis às que são autorizadas por lei, pertinentes e razoavelmente consideradas necessárias para a execução adequada das funções autorizadas da agência» ([176]). Além disso, na medida do razoavelmente praticável, as agências federais devem assegurar que as informações pessoais identificáveis são exatas, pertinentes, atuais e completas e reduzidas ao mínimo necessário para a execução adequada das funções de uma agência. Em termos mais gerais, as agências federais devem estabelecer um programa de privacidade abrangente para garantir o cumprimento dos requisitos de privacidade aplicáveis, desenvolver e avaliar políticas de privacidade e gerir os riscos para a privacidade, manter procedimentos para detetar, documentar e comunicar situações de incumprimento da privacidade, desenvolver programas de sensibilização e formação em matéria de privacidade destinados aos funcionários e contratantes e adotar políticas e procedimentos para assegurar que o pessoal é responsabilizado pelo cumprimento dos requisitos e políticas de privacidade ([177]).

(103) Além disso, a *E-Government Act* ([178]) exige que todas as agências federais (incluindo as autoridades responsáveis pela aplicação do direito penal) apliquem proteções de segurança da informação proporcionais ao risco e à magnitude dos danos que resultariam do acesso, utilização, divulgação, perturbação, alteração ou destruição não autorizados e tenham um *Chief Information Officer* para assegurar o cumprimento dos requisitos de segurança da informação e efetuar uma avaliação anual independente (por exemplo, por um inspetor-geral, ver considerando 109) do seu programa e práticas de segurança da informação ([179]). Do mesmo modo, a *Federal Records Act* (FRA) ([180]) e os regulamentos complementares ([181]) exigem que as informações detidas pelas agências federais estejam sujeitas a garantias que assegurem a integridade física das informações e que as protejam contra o acesso não autorizado.

(104) Em conformidade com a legislação federal, em especial a *Federal Information Security Modernisation Act* de 2014, o OMB e o *National Institute of Standards and Technology* (NIST) desenvolveram normas vinculativas aplicáveis às agências federais (incluindo as autoridades responsáveis pela aplicação do direito penal), que especificam os requisitos mínimos de segurança da informação que têm de ser aplicados, nomeadamente controlos de acesso, garantia da realização de campanhas de sensibilização e de ações de formação, planeamento de contingência, resposta a incidentes, ferramentas de auditoria e responsabilização, garantia da integridade do sistema e da informação, realização de avaliações dos riscos em matéria de privacidade e segurança, etc. ([182]). Além disso, todas

([175]) Ou seja, «informações que podem ser utilizadas para distinguir ou determinar a identidade de uma pessoa, isoladamente ou quando combinadas com outras informações que estejam associadas, ou possam ser associadas, a uma pessoa específica». Ver a Circular n.º A-130 do OMB, p. 33 (definição de «informações pessoais identificáveis»).

([176]) Apêndice II, *Responsibilities for Managing Personally Identifiable Information*, da Circular n.º A-130 do OMB, *Managing Information as a Strategic Resource*, 81 Fed. Reg. 49,689 (28 July 2016), p. 17.

([177]) Apêndice II, § 5(a)-(h).

([178]) 44 U.S.C., capítulo 36.

([179]) 44 U.S.C. §§ 3544-3545.

([180]) FAC, 44 U.S.C. § 3105.

([181]) 36 C.F.R. §§ 1228,150 e seguintes, 1228,228, e apêndice A.

([182]) Ver, por exemplo, a Circular n.º A-130 do OMB, NIST SP 800-53, Rev. 5, *Security and Privacy Controls for Information Systems and Organizations* (10 de dezembro de 2020); e as *Federal Information Processing Standards 200: Minimum Security Requirements for Federal Information and Information Systems* do NIST.

as agências federais (incluindo as autoridades responsáveis pela aplicação do direito penal) devem, em conformidade com as orientações do OMB, manter e aplicar um plano para gerir violações de dados, nomeadamente no que diz respeito à resposta a essas violações e à avaliação dos riscos de danos ([183]).

(105) No que respeita à conservação de dados, a FRA ([184]) exige que as agências federais norte-americanas (incluindo as autoridades responsáveis pela aplicação do direito penal) fixem períodos de conservação para os seus registos (após os quais esses registos devem ser eliminados), que devem ser aprovados pela *National Archives and Record Administration* ([185]). A duração destes períodos de conservação é fixada tendo em conta diferentes fatores, como o tipo de investigação, se as provas ainda são pertinentes para a investigação, etc. No que diz respeito ao FBI, as AGG-DOM estabelecem que o FBI deve ter em vigor um plano de conservação de registos e manter um sistema que permita recuperar rapidamente o estado e a base das investigações.

(106) Por último, a Circular n.º A-130 do OMB também contém determinados requisitos em matéria de divulgação de informações pessoais identificáveis. Em princípio, a divulgação e a comunicação de informações pessoais identificáveis devem limitar-se ao que é legalmente autorizado, pertinente e razoavelmente considerado necessário para o bom desempenho das funções de uma agência ([186]). Quando partilham informações pessoais identificáveis com outras entidades governamentais, as agências federais norte-americanas devem impor, se for caso disso, condições (incluindo a aplicação de controlos de segurança e privacidade específicos) que regulem o tratamento das informações através de acordos escritos (nomeadamente contratos, acordos de utilização de dados, acordos de intercâmbio de informações e memorandos de entendimento) ([187]). No que diz respeito aos motivos com base nos quais as informações podem ser divulgadas, o AGG-DOM e o *Domestic Investigations and Operations Guide* do FBI ([188]), por exemplo, que o FBI pode estar sujeito a uma obrigação legal de o fazer (por exemplo, ao abrigo de um acordo internacional) ou está autorizado a divulgar informações em determinadas circunstâncias, por exemplo, a outras agências dos EUA, se a divulgação for compatível com a finalidade para a qual as informações foram recolhidas e estiver relacionada com as suas responsabilidades; às comissões do Congresso; a agências estrangeiras, se a informação estiver relacionada com as suas responsabilidades e a divulgação for coerente com os interesses dos Estados Unidos; a divulgação for, nomeadamente, necessária para proteger a segurança de pessoas ou bens, ou para proteger ou prevenir um crime ou ameaça à segurança nacional e a sua divulgação for compatível com a finalidade para a qual as informações foram recolhidas ([189]).

3.1.2. ***Supervisão***

(107) As atividades das agências federais responsáveis pela aplicação do direito penal estão sujeitas à supervisão de vários organismos ([190]). Tal como se explica nos considerandos 92 a 99, tal inclui, na maioria dos casos, um controlo judicial prévio para autorizar as medidas de recolha antes de as executar. Além disso, outros organismos supervisionam as diferentes fases das atividades das autoridades responsáveis pela aplicação do direito penal, incluindo a recolha e o tratamento de dados pessoais. Em conjunto, estes organismos judiciais e extrajudiciais asseguram que as autoridades responsáveis pela aplicação da lei estão sujeitas a uma supervisão independente.

([183]) Memorando 17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*, disponível em: https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2017/m-17-12_0.pdf e Circular n.º A-130 do OMB. Por exemplo, para os procedimentos de resposta a violações de dados do *Department of Justice*, *ver*: https://www.justice.gov/file/4336/download.

([184]) FRA, 44 U.S.C. §§ 3101 e seguintes.

([185]) A *National Archives and Record Administration* tem autoridade para avaliar as práticas de gestão de registos das agências e pode determinar se é justificada a conservação contínua de determinados registos [44 U.S.C. §§ 2904(c), 2906].

([186]) Secção 5.f.1.(d) da Circular No. A-130 do OMB.

([187]) Apêndice I § 3(d) da Circular n.º A-130 do OMB.

([188]) Ver também a secção 14 do *Domestic Investigations and Operations Guide* do FBI (DIOG).

([189]) AGG-DOM, secções VI, B e C; *Domestic Investigations and Operations Guide* do FBI (DIOG), secção 14.

([190]) Os mecanismos mencionados na presente secção aplicam-se igualmente à recolha e utilização de dados pelas autoridades federais para fins civis e regulamentares. As agências civis e reguladoras federais estão sujeitas ao controlo dos respetivos diretores-gerais e à supervisão do Congresso, incluindo o *Government Accountability Office*, a agência de auditoria e investigação do Congresso. A menos que a agência tenha um responsável pela proteção da privacidade e das liberdades civis — cargo que normalmente existe em agências como o *Department of Justice* e o *Department of Homeland Security* (DHS) devido às suas responsabilidades em matéria de aplicação da lei e de segurança nacional — estas funções cabem ao responsável superior pela privacidade da agência. Todas as agências federais estão legalmente obrigadas a designar um responsável superior pela privacidade, que assume a responsabilidade de assegurar a conformidade da agência com a legislação em matéria de privacidade e de supervisionar questões que daí decorram. Ver, por exemplo, OMB M-16-24, *Role and Designation of Senior Agency Officials for Privacy* (2016).

(108) Em primeiro lugar, existem agentes responsáveis pela proteção da privacidade e das liberdades cívicas em vários departamentos com responsabilidades no domínio da aplicação do direito penal ([191]). Embora os poderes específicos destes agentes possam variar um pouco em função do estatuto de autorização, habitualmente 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. Os diretores de cada departamento ou serviço devem assegurar que os agentes responsáveis pela proteção da privacidade e das liberdades cívicas dispõem do material e dos recursos necessários para cumprir o seu mandato, têm acesso a todo o material e pessoal necessários para o exercício das suas funções e são informados e consultados sobre as alterações políticas propostas ([192]). Os agentes responsáveis pela proteção da privacidade e das liberdades cívicas comunicam periodicamente ao Congresso, designadamente sobre o número e a natureza das queixas recebidas pelo departamento/organismo, bem como um resumo dessas queixas, as análises efetuadas e as questões colocadas e ainda o impacto das atividades levadas a cabo pelo agente ([193]).

(109) Em segundo lugar, um inspetor-geral independente supervisiona as atividades do *Department of Justice*, incluindo o FBI ([194]). Os inspetores-gerais são juridicamente independentes ([195]) e responsáveis pela realização de investigações, auditorias e inspeções independentes dos programas e operações do departamento. Podem aceder a todos os registos, relatórios, auditorias, revisões, documentos, recomendações ou outros materiais pertinentes, através de intimações, se necessário, e podem recolher depoimentos ([196]). Embora os inspetores-gerais emitam recomendações não vinculativas sobre medidas corretivas, os seus relatórios, em especial sobre medidas de acompanhamento (ou a sua inexistência) ([197]) são geralmente tornados públicos e transmitidos ao Congresso que pode, com base neles, exercer a sua função de supervisão (ver considerando 111) ([198]).

([191]) Ver 42 U.S.C. § 2000ee-1. Tal inclui, por exemplo, o *Department of Justice*, o *Department of Homeland Security* e o FBI. No *Department of Homeland Security*, além disso, o *Chief Privacy Officer* é responsável por preservar e melhorar a proteção da privacidade e promover a transparência no seio do departamento (6 U.S.C. 142, secção 222). Todos os sistemas, tecnologias, formulários e programas do *Department of Homeland Security* que recolhem dados pessoais ou têm um impacto na privacidade estão sujeitos à supervisão do *Chief Privacy Officer*, que tem acesso a todos os registos, relatórios, auditorias, análises, documentos, dossiês, recomendações e outros materiais disponíveis no departamento e, se necessário, por intimação. O *Chief Privacy Officer* tem de apresentar anualmente ao Congresso um relatório sobre as atividades do departamento que afetam a privacidade, incluindo as queixas de violações da privacidade.

([192]) 42 U.S.C. § 2000ee-1(d).

([193]) Ver 42 U.S.C. §§ 2000ee-1 (f)(1)-(2). Por exemplo, o relatório do *Chief Privacy and Civil Liberties Officer* do DOJ e do *Office of Privacy and Civil Liberties*, que abrange o período de outubro de 2020 a março de 2021, mostra que foram efetuadas 389 análises da privacidade, incluindo de sistemas de informação e outros programas (https://www.justice.gov/d9/pages/attachments/2021/05/10/2021-4--21opclsection803reportfy20sa1_final.pdf).

([194]) Do mesmo modo, foi criado, pela*Homeland Security Act* de 2002, o *Office of Inspector General* no *Department of Homeland Security* .

([195]) O cargo dos inspetores-gerais é assegurado e só podem ser destituídos pelo Presidente, que deve comunicar ao Congresso, por escrito, os motivos da destituição.

([196]) Ver *Inspector General Act* de 1978, § 6.

([197]) Ver, a este respeito, por exemplo, o resumo preparado pelo *Office of the Inspector General* do DoJ sobre as recomendações formuladas e a medida em que foram implementadas através de medidas de acompanhamento do departamento e do serviço, https://oig.justice.gov/sites/default/files/reports/22-043.pdf.

([198]) Ver *Inspector General Act* de 1978, §§ 4(5), 5. Por exemplo, o *Office of the Inspector General* do *Department of Justice* publicou recentemente o seu relatório semestral ao Congresso (de 1 de outubro de 2021 a 31 de março de 2022, https://oig.justice.gov/node/23596), que apresenta uma panorâmica das suas auditorias, avaliações, inspeções, análises especiais e investigações dos programas e operações do DOJ. Estas atividades incluíram uma investigação de um antigo contratante sobre a divulgação ilegal de conteúdo de vigilância eletrónica (escutas de um cidadão) numa investigação em curso, que conduziu à condenação do contratante. O *Office of the Inspector General* conduziu também uma investigação dos programas e práticas de segurança da informação das agências do DOJ, que inclui o teste da eficácia das políticas, procedimentos e práticas de segurança da informação de um subconjunto representativo dos sistemas das agências.

(110) Em terceiro lugar, na medida em que levam a cabo atividades de luta contra o terrorismo, os departamentos com responsabilidades em matéria de aplicação do direito penal estão sujeitos à supervisão do *Privacy and Civil Liberties Oversight Board* (PCLOB), uma agência independente do poder executivo composta por um conselho bipartidário de cinco membros nomeados pelo Presidente por um mandato fixo de seis anos com aprovação do Senado ([199]). De acordo com o seu estatuto constitutivo, a PCLOB tem responsabilidades no domínio das políticas de luta contra o terrorismo e da sua aplicação, com vista à proteção da privacidade e das liberdades cívicas. Na sua análise, pode aceder a todos os registos, relatórios, auditorias, análises, documentos e recomendações dos serviços de informações pertinentes, nomeadamente informações classificadas, realizar entrevistas e recolher depoimentos ([200]). Recebe relatórios dos agentes responsáveis pela proteção da privacidade e das liberdades cívicas de vários departamentos/serviços federais ([201]), pode emitir recomendações às autoridades governamentais e às autoridades responsáveis pela aplicação da lei, e informa regularmente os comités do Congresso e ao Presidente ([202]). Os relatórios do conselho, incluindo os que são apresentados ao Congresso, devem ser, na medida do possível, disponibilizados ao público ([203]).

(111) Por último, as atividades de aplicação do direito penal estão sujeitas à supervisão de comités específicos do Congresso dos EUA (os *House and Senate Judiciary Committees*). Os *Judiciary Committees* exercem uma supervisão regular de diferentes formas, nomeadamente através de audições, investigações, análises e relatórios ([204]).

3.1.3. ***Reparação***

(112) Tal como referido, as autoridades responsáveis pela aplicação do direito penal devem, na maioria dos casos, obter uma autorização judicial prévia para recolher dados pessoais. Embora tal não seja exigido para as intimações administrativas, estas são limitadas a situações específicas e estão sujeitas a um controlo jurisdicional independente, pelo menos quando o governo procura obter a sua aplicação em tribunal. Em especial, os destinatários de intimações administrativas podem contestá-las em tribunal alegando que não são razoáveis, ou seja, que são demasiado abrangentes, opressivas ou onerosas ([205]).

(113) As pessoas singulares podem, em primeiro lugar, apresentar pedidos ou queixas às autoridades responsáveis pela aplicação do direito penal relativamente ao tratamento dos seus dados pessoais. Aqui se inclui a possibilidade de solicitar o acesso aos dados pessoais e a sua correção ([206]). No que diz respeito às atividades relacionadas com a luta contra o terrorismo, as pessoas singulares podem também apresentar queixa junto dos responsáveis pela proteção da privacidade e das liberdades cívicas (ou outros funcionários responsáveis pela proteção da privacidade) junto das autoridades responsáveis pela aplicação da lei ([207]).

(114) Além disso, a legislação dos EUA prevê um certo número de vias de recurso judiciais para os cidadãos, contra as autoridades públicas ou um dos seus funcionários, quando estas autoridades tratam dados pessoais ([208]). Estas vias, que incluem especialmente a APA, a *Freedom of Information Act* (FOIA) e a *Electronic Communications Privacy Act* (ECPA), estão abertas a todos cidadãos independentemente da sua nacionalidade, sem prejuízo de quaisquer condições aplicáveis.

([199]) Os membros do conselho devem ser selecionados exclusivamente com base nas suas qualificações profissionais, realizações, estatuto público, conhecimentos especializados em matéria de liberdades cívicas e privacidade e experiência relevante, sem ter em conta a sua filiação política. Em caso algum pode haver mais de três membros do conselho filiados no mesmo partido político. Uma pessoa nomeada para o conselho não pode, enquanto exercer funções no conselho, ser um funcionário eleito, um agente ou um funcionário do governo federal, exceto na qualidade de membro do conselho. Ver 42 U.S.C. § 2000ee h).

([200]) 42 U.S.C. § 2000ee g).

([201]) Ver 42 U.S.C. § 2000ee-1 (f)(1)(A)(iii). Estes incluem, pelo menos, o *Department of Justice*, o *Department of Defense* e o *Department of Homeland Security*, para além de qualquer outro departamento, agência ou elemento do poder executivo que seja designado que a PCLOB considere pertinente.

([202]) 42 U.S.C. §2000ee, (e).

([203]) 42 U.S.C. § 2000ee (f).

([204]) Por exemplo, os comités organizam audições temáticas (ver, a título de exemplo, uma audição recente do *House Judiciary Committee* sobre «redes de arrasto digitais»), https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4983), bem como audições regulares de supervisão, por exemplo, do FBI e do DOJ, ver: https://www.judiciary.senate.gov/meetings/08/04/2022/oversight-of-the-federal--bureau-of-investigation; https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4966 e https://judiciary.house.gov/calendar/ /eventsingle.aspx?EventID=4899.

([205]) Ver anexo VI.

([206]) Circular n.º A-130, apêndice II, secção 3, alíneas a) e f), do OMB, que impõe às agências federais a obrigação de assegurarem um acesso adequado e a correção solicitada pelas pessoas singulares, e estabelecerem procedimentos para receber e tratar queixas e pedidos relacionados com a privacidade.

([207]) Ver 42 U.S.C. § 2000e-1 no que diz respeito, por exemplo, ao DoJ e ao *Department of Homeland Security*. Ver tambémMemorandum M-16-24 do OMB, *Role and Designation of Senior Agency Officials for Privacy*.

([208]) Os mecanismos de recurso mencionados na presente secção aplicam-se igualmente à recolha e utilização de dados pelas autoridades federais para fins civis e regulamentares.

(115) Em geral, nos termos das disposições relativas a um recurso judicial da APA, ([209]) 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 ([210]). 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» ([211]).

(116) Mais especificamente, o título II da ECPA ([212]) 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 ([213]). Criminaliza o acesso ilegal (ou seja, não autorizado pelo tribunal ou admissível de outro modo) a essas comunicações e prevê que um cidadão que se considere lesado possa intentar uma ação cível num tribunal federal dos EUA para obter reparação por perdas e danos, bem como uma compensação equitativa contra um funcionário do governo que tenha cometido intencionalmente esses atos ilegais, ou contra os Estados Unidos.

(117) Além disso, várias outras leis garantem aos cidadãos o direito de intentar um processo contra uma autoridade pública ou um funcionário americano no que diz respeito ao tratamento dos seus dados pessoais, como a *Wiretap Act* ([214]), a *Computer Fraud and Abuse Act* ([215]), a *Federal Torts Claim Act* ([216]), a *Right to Financial Privacy Act* ([217]), e a *Fair Credit Reporting Act* ([218]).

([209]) 5 U.S.C. § 702.

([210]) 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.

([211]) 5 U.S.C. § 706(2)(A).

([212]) 18 U.S.C. §§ 2701-2712.

([213]) 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 o serviço informático de aramazenamento ou tratamento de dados.

([214]) 18 U.S.C. §§ 2510 e seg. Nos termos 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 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).

([215]) 18 U.S.C. § 1030. Nos termos da Computer Fraud and Abuse Act, qualquer cidadão 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 norte-americanas ou de um outro sistema específico, incluindo, em certas circunstâncias, contra um funcionário do governo.

([216]) 28 U.S.C. §§ 2671 e seg. Nos termos 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.»

([217]) 12 U.S.C. §§ 3401 e seg. Nos termos 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 o cidadão, relativamente ao qual são solicitadas informações, receba notificação do pedido.

([218]) 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.

(118) Além disso, nos termos da FOIA ([219]), 5 U.S.C. § 552, qualquer pessoa tem o direito de obter acesso aos registos das agências federais, incluindo quando estes contenham os dados da pessoa em causa. Depois de esgotadas as vias de recurso administrativas, uma pessoa pode invocar esse direito de acesso em tribunal, a menos que esses registos estejam protegidos contra a divulgação pública por uma isenção ou uma exclusão especial das autoridades responsáveis pela aplicação da lei ([220]). Neste caso, o tribunal apreciará se alguma isenção se aplica ou se foi legalmente invocada pela autoridade pública competente.

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

(119) O direito da dos Estados Unidos contém várias limitações e garantias no que respeita ao acesso e à utilização de dados pessoais para efeitos de segurança nacional, e prevê mecanismos de recurso e supervisão neste domínio, que estão em conformidade com os requisitos referidos no considerando 89 da presente decisão. Os pontos seguintes descrevem as condições nas quais esse acesso pode ser efetuado e as garantias aplicáveis à utilização desses poderes.

3.2.1. ***Bases jurídicas, limitações e garantias***

3.2.1.1 *Quadro jurídico aplicável*

(120) Os dados pessoais transferidos da União para as organizações do QPD UE-EUA podem ser recolhidos pelas autoridades norte-americanas para fins de segurança nacional com base em diferentes instrumentos jurídicos, sob reserva de condições e garantias específicas.

(121) Uma vez recebidos dados pessoais por organizações localizadas nos Estados Unidos, os serviços de informações dos EUA só podem solicitar o acesso a esses dados para fins de segurança nacional se tal for autorizado por lei, especificamente ao abrigo da *Foreign Intelligence Surveillance Act* (FISA) ou de disposições legais que autorizem o acesso mediante requerimentos de segurança nacional (*National Security Letters*) ([221]). A FISA contém várias bases jurídicas que podem ser utilizadas para recolher (e posteriormente tratar) os dados pessoais de titulares dos dados da União transferidos no âmbito do QPD UE-EUA (secção 105 ([222]) da FISA, secção 302 da FISA ([223]), secção 402 da FISA ([224]), secção 501 da FISA ([225]) e secção 702 da FISA ([226])), tal como descrito mais circunstanciadamente nos considerandos 135 a 152.

([219]) 5 U.S.C. § 552.

([220]) Estas exclusões são, contudo, enquadradas. Por exemplo, em conformidade com o 5 U.S.C. § 552 (b)(7), os direitos atribuídos nos termos da FOIA são excluídos para os «documentos ou informações recolhidos para efeitos de aplicação da lei, mas apenas na medida em que a apresentação desses documentos ou informações em matéria de aplicação da lei: A) possa razoavelmente ser considerada uma ingerência no processo de execução, B) prive um cidadão do direito a um processo equitativo ou a um julgamento imparcial, C) possa razoavelmente ser considerada como constituindo uma invasão injustificada da vida privada, D) possa 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 tenha fornecido informações a título confidencial e, no caso de um documento ou de informações recolhidas pelas autoridades responsáveis pela aplicação do direito penal no decurso de uma investigação penal ou por uma agência que conduza uma investigação nacional legal em matéria de informações de segurança, informações fornecidas por uma fonte confidencial, E) tenha por efeito divulgar as técnicas e os procedimentos das investigações e das ações penais ou as orientações aplicáveis às investigações ou às ações penais intentadas pelas autoridades responsáveis pela aplicação da lei, se se puder razoavelmente esperar que essa divulgação contornaria a lei, ou F) possa pôr em perigo a vida ou a segurança física de um cidadão». 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 tem conhecimento 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)].

([221]) 12 U.S.C. § 3414; 15 U.S.C. §§ 1681u-1681v; e 18 U.S.C. § 2709. Ver considerando 153.

([222]) 50 U.S.C. § 1804, que diz respeito à vigilância eletrónica individualizada convencional.

([223]) 50 U.S.C. § 1822, que diz respeito a buscas físicas para efeitos de informações externas.

([224]) 50 U.S.C. § 1842 com § 1841(2) e título 18, secção 3127, que diz respeito à instalação de dispositivos de registo de chamadas telefónicas e comunicações eletrónicas.

([225]) 50 U.S.C. § 1861, que permite ao FBI apresentar «um pedido de decisão que autorize uma empresa de transportes públicos, uma unidade de alojamento pública, uma instalação de armazenamento físico ou um estabelecimento de aluguer de veículos a apresentar documentação na sua posse para uma investigação destinada a recolher informações externas ou uma investigação relativa a terrorismo internacional».

([226]) 50 U.S. Code § 1881a, que permite que os elementos do setor norte-americano das informações solicitem o acesso a informações, nomeadamente ao conteúdo de comunicações na Internet, de empresas norte-americanas, visando determinados cidadãos de países terceiros fora dos Estados Unidos, com a assistência legalmente obrigatória dos prestadores de serviços de comunicações eletrónicas.

(122) Os serviços de informações dos EUA também têm a possibilidade de recolher dados pessoais fora dos Estados Unidos, que podem incluir dados pessoais em trânsito entre a União e os Estados Unidos. A recolha fora dos Estados Unidos baseia-se no *Executive Order 12333* (EO 12333) ([227]), emitido pelo Presidente ([228]).

(123) A recolha de informação de origem eletromagnética é a forma de recolha de informações mais relevante para a presente verificação de adequação, uma vez que diz respeito à recolha de comunicações eletrónicas e de dados de sistemas de informação. Essa recolha pode ser efetuada pelos serviços de informações dos EUA nos Estados Unidos (com base na FISA) e enquanto os dados estão em trânsito para os Estados Unidos (com base no EO 12333).

(124) Em 7 de outubro de 2022, o presidente dos EUA emitiu o EO 14086 sobre o reforço das garantias para a informação de origem eletromagnética dos Estados Unidos, que estabelece limitações e garantias aplicáveis a todas as atividades de informação de origem eletromagnética dos EUA. O EO substitui, em grande medida, a *Presidential Policy Directive* (PPD 28) ([229]), reforça as condições, as limitações e as garantias aplicáveis a todas as atividades de informação de origem eletromagnética (isto é, com base na FISA e no EO 12333), independentemente do local onde tenham lugar ([230]), e cria um novo mecanismo de recurso através do qual os cidadãos ([231]) podem invocar e aplicar estas garantias (ver informações mais pormenorizadas nos considerandos 176 a 194). Ao fazê-lo, transpõe, para o direito dos EUA, o resultado das conversações que tiveram lugar entre a UE e os EUA na sequência da invalidação da decisão de adequação da Comissão relativa ao Escudo de Proteção da Privacidade pelo Tribunal de Justiça (ver considerando 6), pelo que é um elemento particularmente importante do quadro jurídico avaliado na presente decisão.

(125) As limitações e salvaguardas introduzidas pelo EO 14086 complementam as previstas na secção 702 do FISA e na secção 12333 do EO. Os requisitos a seguir descritos (nas secções 3.2.1.2 e 3.2.1.3) devem ser aplicados pelos serviços de informações quando realizam atividades de informação de origem eletromagnética nos termos da secção 702 da FISA e da secção 12333 do EO, por exemplo, quando selecionam/identificam categorias de informações estrangeiras a obter nos termos da secção 702 da FISA; quando recolhem informações estrangeiras ou de contraespionagem nos termos do EO 12333; e quando tomam decisões de seleção de objetivos individuais ao abrigo da secção 702 da FISA e da secção 12333 do EO.

(126) Os requisitos estabelecidos neste decreto executivo emitido pelo Presidente são vinculativos para todo o setor das informações. Devem ser aplicadas ainda através de políticas e procedimentos das agências que os transponham para orientações concretas aplicáveis às operações quotidianas. A este respeito, o EO 14086 concede aos serviços de informações dos EUA um prazo máximo de um ano para atualizar as suas políticas e procedimentos em vigor (ou seja, até 7 de outubro de 2023), a fim de os tornar conformes com os requisitos constantes do decreto executivo. Essas políticas e procedimentos atualizados têm de ser desenvolvidos em consulta com o *Attorney General*, com o *Civil Liberties Protection Officer* do *Office of the Director of National Intelligence* (CLPO do ODNI) e com a PCLOB — um organismo de supervisão independente autorizado a analisar as políticas do poder executivo e a sua aplicação, com vista a proteger a privacidade e as liberdades cívicas (ver considerando 110 no que se refere ao papel e ao estatuto da PCLOB) — e disponibilizados ao público ([232]). Além disso, quando as políticas e os procedimentos atualizados

([227]) EO 12333: *United States Intelligence Activities*, *Federal Register*, vol. 40, n.º 235 (8 de dezembro de 1981, com a redação que lhe foi dada em 30 de julho de 2008). O EO 12333 define de forma mais geral os objetivos, as orientações, as funções 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.

([228]) Nos termos do artigo II da Constituição dos EUA, a responsabilidade de garantir a segurança nacional, incluindo, em especial, a recolha de informações externas, é da competência do Presidente enquanto Comandante Supremo das Forças Armadas.

([229]) O EO 14086 substitui uma diretiva presidencial anterior, a PPD 28, com exceção da sua secção 3 e de um anexo complementar (que exige que os serviços de informações revejam anualmente as suas prioridades e requisitos em matéria de informação de origem eletromagnética, tendo em conta os benefícios das atividades de informação de origem eletromagnética para os interesses nacionais dos EUA, bem como o risco que essas atividades representam) e da secção 6 (que contém disposições gerais). Ver o *National Security Memorandum on Partial Revocation of Presidential Policy Directive 28*, disponível em: https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/07/national-security-memorandum-on-partial-revocation-of-presidential-policy-directive-28/.

([230]) Ver secção 5(f) do EO 14086, que explica que o decreto executivo tem o mesmo âmbito de aplicação que a PPD 28, que, de acordo com a sua nota de rodapé 3, era aplicável às atividades de informação de origem eletromagnética realizadas para recolher comunicações ou informações sobre comunicações, exceto as atividades de informação de origem eletromagnética realizadas para testar ou desenvolver capacidades em matéria de informação de origem eletromagnética.

([231]) Ver, a este respeito, por exemplo, a secção 5(h) do EO 14086, que esclarece que as garantias previstas no decreto executivo criam um direito legal e podem ser aplicadas pelos cidadãos através do mecanismo de recurso.

([232]) Ver secção 2(c)(iv)(C) do EO 14086.

estiverem em vigor, a PCLOB procederá a uma análise para garantir a sua coerência com o decreto executivo. No prazo de 180 dias após a conclusão dessa análise pela PCLOB, cada serviço de informações deve considerar cuidadosamente todas as recomendações formuladas pela PCLOB e aplicá-las ou, de outro modo, dar-lhes resposta . Em 3 de julho de 2023, o Governo dos EUA publicou essas políticas e procedimentos atualizados ([233]).

3.2.1.2 *Limitações e garantias no que respeita à recolha de dados pessoais para fins de segurança nacional*

(127) O EO 14086 estabelece uma série de ambiciosos requisitos aplicáveis a todas as atividades de informação de origem eletromagnética (recolha, utilização, divulgação, etc. de dados pessoais).

(128) Em primeiro lugar, essas atividades devem basear-se numa lei ou numa autorização presidencial e ser realizadas em conformidade com o direito dos EUA, nomeadamente a Constituição ([234]).

(129) Em segundo lugar, devem existir garantias adequadas para assegurar que a privacidade e as liberdades cívicas são considerações integrais no planeamento de tais atividades ([235]).

(130) Em especial, qualquer atividade de informação de origem eletromagnética só pode ser realizada «após a determinação, com base numa avaliação razoável de todos os fatores pertinentes, de que as atividades são necessárias para promover uma prioridade em matéria de informações validada» (no que se refere ao conceito de «prioridade em matéria de informações validada», ver considerando 135) ([236]).

(131) Além disso, tais atividades só podem ser realizadas «na medida e de uma forma que seja proporcional à prioridade em matéria de informações validada para a qual foram autorizadas» ([237]). Dito de outro modo, deve alcançar-se um equilíbrio adequado «entre a importância da prioridade em matéria de informações perseguida e o impacto na privacidade e nas liberdades cívicas dos cidadãos afetados, independentemente da sua nacionalidade ou do local onde residam» ([238]).

(132) Por último, para assegurar o respeito destes requisitos gerais — que refletem os princípios da legalidade, da necessidade e da proporcionalidade — as atividades de informação de origem eletromagnética estão sujeitas a supervisão (ver informações mais pormenorizadas na secção 3.2.2) ([239]).

(133) Estes requisitos abrangentes são fundamentados mais aprofundadamente no que diz respeito à recolha de informação de origem eletromagnética através de uma série de condições e limitações que asseguram que a ingerência nos direitos dos cidadãos se limita ao necessário e proporcionado para promover um objetivo legítimo.

(134) Em primeiro lugar, o decreto executivo limita de duas formas os motivos segundo os quais os dados podem ser recolhidos no âmbito das atividades de informação de origem eletromagnética. Por um lado, o decreto executivo fixa os objetivos legítimos suscetíveis de serem concretizados através da recolha de informação de origem eletromagnética, por exemplo, para compreender ou avaliar as capacidades, intenções ou atividades de organizações estrangeiras, nomeadamente organizações terroristas internacionais, que representem uma ameaça atual ou potencial para a segurança nacional dos Estados Unidos, proteger contra capacidades e atividades militares estrangeiras, compreender ou avaliar as ameaças transnacionais que afetam a segurança mundial, como as alterações climáticas e outras alterações ecológicas, riscos para a saúde pública e ameaças humanitárias ([240]). Por outro lado, o

([233]) https://www.intel.gov/ic-on-the-record-database/results/oversight/1278-odni-releases-ic-procedures-implementing-new-safeguards--in-executive-order-14086.

([234]) Secção 2(a)(i) do EO 14086.

([235]) Secção 2(a)(ii) do EO 14086.

([236]) Secção 2(a)(ii)(A) do EO 14086. Tal nem sempre exige que a informação de origem eletromagnética seja o único meio para promover os aspetos de uma prioridade em matéria de informações validada. Por exemplo, a recolha de informação de origem eletromagnética pode ser utilizada para assegurar vias alternativas de validação (por exemplo, para corroborar as informações recebidas de outras fontes de informações) ou para manter um acesso fiável às mesmas informações [secção 2(c)(i)(A) do EO 14086].

([237]) Secção 2(a)(ii)(B) do EO 14086.

([238]) Secção 2(a)(ii)(B) do EO 14086.

([239]) Secção 2(a)(iii) em conjugação com a secção 2(d) do EO 14086.

([240]) Secção 2(b)(i) do EO 14086. Devido à lista circunscrita de objetivos legítimos estabelecidos no EO, que não abrange eventuais ameaças futuras, o EO contempla a possibilidade de o Presidente atualizar essa lista caso surjam novos imperativos de segurança nacional, tais como novas ameaças à segurança nacional. Essas atualizações devem, em princípio, ser divulgadas publicamente, a menos que o presidente determine que tal representa, por si só, um risco para a segurança nacional dos Estados Unidos [secção 2(b)(i)(B) do EO 14086].

decreto executivo enumera determinados objetivos que nunca devem ser concretizados através de atividades de informação de origem eletromagnética, por exemplo, com o objetivo de reprimir críticas, dissidências ou a livre expressão de ideias ou de opiniões políticas por parte dos cidadãos ou da imprensa, com o objetivo de prejudicar os cidadãos com base na sua etnia, raça, sexo, identidade de género, orientação sexual ou religião ou para proporcionar uma vantagem concorrencial às empresas norte-americanas ([241]).

(135) Além disso, os objetivos legítimos estabelecidos no EO 14086 não podem, por si só, ser invocados pelos serviços de informações para justificar a recolha de informação de origem eletromagnética, devendo ser fundamentados mais aprofundadamente, para fins operacionais, em prioridades mais concretas para as quais seja permitida a recolha de informação de origem eletromagnética. Dito de outro modo, a recolha efetiva só pode ter lugar para promover uma prioridade mais específica. Essas prioridades são definidas através de um processo específico destinado a garantir a conformidade com os requisitos legais aplicáveis, nomeadamente os relacionados com a privacidade e as liberdades cívicas. Mais especificamente, as prioridades em matéria de informações são, em primeiro lugar, desenvolvidas pelo *Director of National Intelligence* (através do chamado *National Intelligence Priorities Framework*) e apresentadas ao Presidente para aprovação ([242]). Antes de propor as prioridades em matéria de informações ao Presidente, o diretor deve, em conformidade com o EO 14086, obter uma avaliação do CLPO do ODNI para cada uma das prioridades, a fim de determinar se: 1) promove um ou mais objetivos legítimos enumerados no EO; 2) não foi concebida nem se prevê que venha a resultar na recolha de informação de origem eletromagnética para um objetivo proibido enumerado no decreto executivo; e 3) foi definida após ponderação adequada da privacidade e das liberdades cívicas de todos os cidadãos, independentemente da sua nacionalidade ou do local onde residam ([243]). Se o diretor não concordar com a avaliação do CLPO, ambos os pontos de vista devem ser apresentados ao Presidente ([244]).

(136) Por conseguinte, este processo garante, nomeadamente, que as considerações em matéria de privacidade são tidas em conta desde a fase inicial em que são desenvolvidas as prioridades em matéria de informações.

(137) Em segundo lugar, uma vez definida uma prioridade em matéria de informações, há uma série de requisitos que regem a decisão sobre se, e em que medida, pode ser recolhida informação de origem eletromagnética para promover essa prioridade. Estes requisitos operacionalizam as normas gerais de necessidade e proporcionalidade previstas na secção 2(a) do decreto executivo.

(138) Em especial, a informação de origem eletromagnética só pode ser recolhida «após a determinação, com base numa avaliação razoável de todos os fatores pertinentes, de que a recolha é necessária para promover uma prioridade específica em matéria de informações» ([245]). Aquando da determinação da necessidade de levar a cabo uma atividade de recolha de informação de origem eletromagnética específica com vista a promover uma prioridade em matéria de informações validada, os serviços de informações dos EUA devem considerar a disponibilidade, a viabilidade e a adequação de outras fontes e métodos menos intrusivos, incluindo de fontes diplomáticas e públicas ([246]). Quando disponíveis, deve ser dada prioridade a essas fontes e métodos alternativos e menos intrusivos ([247]).

(139) Quando, na aplicação desses critérios, a recolha de informação de origem eletromagnética for considerada necessária, deve ser «tão seletiva quanto possível» e «não pode ter repercussões desproporcionadas na privacidade e nas liberdades cívicas» ([248]). Para assegurar que a privacidade e as liberdades cívicas não são afetadas de forma desproporcionada — ou seja, para estabelecer um equilíbrio adequado entre as necessidades de segurança nacional e a proteção da privacidade e das liberdades cívicas — há que ter devidamente em conta todos os fatores, como a natureza do objetivo perseguido, o caráter intrusivo da atividade de recolha, incluindo a sua duração, o contributo provável da recolha para o objetivo perseguido, as consequências razoavelmente previsíveis para os cidadãos e a natureza e sensibilidade dos dados a recolher ([249]).

([241]) Secção 2(b)(ii) do EO 14086.
([242]) Secção 102A da *National Security Act* e secção 2(b)(iii) do EO 14086.
([243]) Em casos excecionais (em especial quando esse processo não puder ser realizado devido à necessidade de dar resposta a um requisito em matéria de informações novo ou em desenvolvimento), o Presidente ou o diretor de um elemento do setor das informações pode determinar diretamente essas prioridades, que, em princípio, tem de aplicar os mesmos critérios que os descritos secção 2(b)(iii)(A)(1)-(3). Ver secção 4(n) do EO 14086.
([244]) Secção 2(b)(iii)(C) do EO 14086.
([245]) Secção 2(b) e (c)(i)(A) do EO 14086.
([246]) Secção 2(c)(i)(A) do EO 14086.
([247]) Secção 2(c)(i)(A) do EO 14086.
([248]) Secção 2(c)(i)(B) do EO 14086.
([249]) Secção 2(c)(i)(B) do EO 14086.

(140) Em relação ao tipo de recolha de informação de origem eletromagnética, a recolha de dados nos Estados Unidos, que é a mais relevante para a presente verificação de adequação, uma vez que diz respeito a dados que foram transferidos para organizações localizadas nos EUA, deve ser sempre seletiva, conforme explicado mais circunstanciadamente nos considerandos 142 a 153.

(141) A «recolha em larga escala» ([250]) só é possível fora dos Estados Unidos, com base no EO 12333. Também neste caso, nos termos do EO 14086, deve ser dada prioridade à recolha seletiva ([251]). Inversamente, a recolha em larga escala só é permitida quando a informação necessária para promover uma prioridade em matéria de informações validada não pode ser razoavelmente obtida através da recolha seletiva ([252]). Sempre que seja necessário proceder à recolha em larga escala de dados fora dos Estados Unidos, aplicam-se garantias específicas nos termos do EO 14086 ([253]). Em primeiro lugar, devem ser aplicados métodos e medidas técnicas a fim de limitar os dados recolhidos apenas ao necessário para promover uma prioridade em matéria de informações validada, minimizando simultaneamente a recolha de informações que não são pertinentes ([254]). Em segundo lugar, o decreto executivo limita a utilização da informação recolhida em larga escala (incluindo a consulta) a seis objetivos específicos, a saber, a proteção contra o terrorismo, a tomada de reféns e a manutenção de pessoas em cativeiro por um governo, organização ou cidadão estrangeiros ou em nome de um governo, organização ou cidadão estrangeiros, a proteção contra a espionagem, a sabotagem ou o assassínio internacional, a proteção contra ameaças decorrentes do desenvolvimento, posse ou proliferação de armas de destruição maciça ou de tecnologias e ameaças conexas, etc. ([255]). Por último, qualquer consulta de informação de origem eletromagnética obtida em larga escala só pode ter lugar quando for necessária para promover uma prioridade em matéria de informações validada, na consecução destes seis objetivos e de acordo com as políticas e os procedimentos que tenham devidamente em conta o impacto das consultas na privacidade e nas liberdades cívicas de todos os cidadãos, independentemente da sua nacionalidade ou do local onde residam ([256]).

(142) Para além dos requisitos constantes do EO 14086, a recolha de informação de origem eletromagnética que tenha sido transferida para uma organização localizada nos Estados Unidos está sujeita a limitações e garantias específicas regidas pela secção 702 da FISA ([257]). A secção 702 da FISA permite que se visem cidadãos de países terceiros que se acredita estarem localizados fora dos Estados Unidos, com a assistência obrigatória dos prestadores norte-americanos de serviços de comunicações eletrónicas, para recolher informações externas ([258]). A fim de recolher informações externas nos termos da secção 702 da FISA, o *Attorney General* e o *Director of National Intelligence* apresentam certificações anuais ao *Foreign Intelligence Surveillance Court* (FISC) em que constam as categorias de

([250]) Ou seja, a recolha de grandes quantidades de informação de origem eletromagnética que, por motivos técnicos ou operacionais, são obtidas sem recurso a discriminantes (por exemplo, sem recurso a identificadores ou termos de seleção específicos). Ver secção 4(b) do EO 14086. Nos termos do EO 14086, e conforme explicado mais circunstanciadamente no considerando 141, a recolha em larga escala ao abrigo do EO 12333 só tem lugar quando for necessária para promover prioridades específicas em matéria de informações validadas, estando sujeita a uma série de limitações e garantias destinadas a assegurar que o acesso aos dados não é efetuado de forma indiscriminada. Por conseguinte, a recolha em larga escala deve ser comparada com a recolha efetuada generalizada e indiscriminadamente («vigilância em larga escala») sem limitações e garantias.

([251]) Secção 2(c)(ii)(A) do EO 14086.

([252]) Secção 2(c)(ii)(A) do EO 14086.

([253]) As regras específicas relativas à recolha em larga escala previstas no EO 14086 também se aplicam a uma atividade de recolha de informações de origem eletromagnética seletiva que utiliza temporariamente dados obtidos sem recurso a discriminantes (por exemplo, sem recurso a identificadores ou termos de seleção específicos), ou seja, em larga escala (que só é possível fora do território dos Estados Unidos). Este não é o caso quando esses dados só são utilizados para contribuir para a fase técnica inicial da atividade de recolha de informações de origem eletromagnética, conservadas apenas durante um curto período de tempo necessário para concluir esta fase e apagadas imediatamente após essa fase [secção 2, alínea c), subalínea ii), ponto D), EO 14086]. Neste caso, o único objetivo da recolha inicial sem recurso a discriminantes é permitir uma recolha seletiva de informações através da aplicação de um identificador ou critério de seleção específico. Neste contexto, só os dados que respondam à aplicação de um determinado discriminante são inscritos nas bases de dados do governo, sendo os restantes dados eliminados. Por conseguinte, esta recolha seletiva continua a ser regida pelas regras gerais aplicáveis à recolha de informação de origem eletromagnética, nomeadamente a secção 2(a)-(b) e 2(c)(i) do EO 14086.

([254]) Secção 2(c)(ii)(A) do EO 14086.

([255]) Secção 2(c)(ii)(B) do EO 14086. No caso de emergência de novos imperativos de segurança nacional, como novas ameaças à segurança nacional, o Presidente pode atualizar esta lista. Essas atualizações devem, em princípio, ser divulgadas publicamente, a menos que o Presidente determine que essa publicação representa, por si só, um risco para a segurança nacional dos Estados Unidos [secção 2(c)(ii)(C) do EO 14086]. No que diz respeito às consultas de dados recolhidos em larga escala, ver secção 2(c)(iii)(D) do EO 14086.

([256]) Secção 2(a)(ii)(A) em conjugação com a secção 2(c)(iii)(D) do EO 14086. Ver também anexo VII.

([257]) 50 U.S.C. § 1881.

([258]) 50 U.S.C. § 1881a (a). Em especial, tal como referido pela PCLOB, a vigilância da secção 702 «consiste exclusivamente em visar cidadãos [de países terceiros] específicos sobre os quais foi feita uma determinação individualizada» (*Privacy and Civil Liberties Oversight Board, Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*, 2 de julho de 2014, *Section 702 Report*, p. 111). Ver ainda *NSA CLPO, NSA's Implementation of Foreign Intelligence Act* Section 702, 16.4.2014. O termo «prestador de serviços de comunicações eletrónicas» está definido em 50 U.S.C. § 1881 (a)(4).

informações externas a obter ([259]). As certificações devem ser acompanhadas de procedimentos de orientação, minimização e consulta de informação, que também são aprovados pelo Tribunal e juridicamente vinculativos para os serviços de informações dos EUA .

(143) O FISC é um tribunal independente ([260]) criado por uma lei federal cujas decisões podem ser objeto de recurso para o *Foreign Intelligence Surveillance Court of Review* (FISCR) ([261]) e, em última instância, para o Supremo Tribunal dos Estados Unidos ([262]). O FISC (e o FISCR) são apoiados por um grupo permanente composto por cinco advogados e cinco peritos técnicos com conhecimentos especializados em questões de segurança nacional e liberdades cívicas ([263]). A partir deste grupo, o tribunal nomeia um cidadão 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, salvo se o tribunal considerar que essa nomeação não é adequada ([264]). Em especial, tal garante que as considerações em matéria de proteção da privacidade são tidas em devida conta na avaliação do tribunal. O tribunal também pode nomear um cidadão ou organização para intervir na qualidade de *amicus curiae*, nomeadamente para fornecer competências técnicas, sempre que considere necessário ou, mediante proposta, autorizar uma pessoa ou organização a apresentar informações a título de *amicus curiae* ([265]).

(144) O FISC aprecia as certificações e os procedimentos conexos (em especial os procedimentos de orientação e minimização) para verificar a conformidade com os requisitos constantes da FISA. Se considerar que os requisitos não estão a ser cumpridos, pode recusar total ou parcialmente a certificação e solicitar a alteração dos procedimentos ([266]). A este respeito, o FISC tem confirmado repetidamente que a sua apreciação dos procedimentos de orientação e minimização previstos na secção 702 não se limita aos procedimentos tal como estão redigidos, mas inclui também a forma como os procedimentos são aplicados pelo governo ([267]).

(145) As decisões sobre a seleção de alvos individuais são feitas pela *National Security Agency* (NSA, o serviço de informações responsável pela seleção de alvos nos termos da secção 702 da FISA) de acordo com os procedimentos de seleção de alvos aprovados pelo FISC, que exigem que a NSA avalie, tendo em conta todas as circunstâncias, que a seleção de um cidadão específico é suscetível de conduzir à obtenção de uma categoria de informações externas constantes de uma certificação ([268]). Esta avaliação deve ser particularizada e baseada em factos, fundamentada por

([259]) 50 U.S.C. § 1881a (g).

([260]) O FISC é constituído por juízes nomeados pelo *Chief Justice* de entre os 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 50 U.S.C. § 1803 (a). 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 ofício 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, disponível em https://fas.org/irp/news/2013/07/fisc-leahy.pdf.

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

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

([263]) 50 U.S.C. § 1803 (i)(1),(3)(A).

([264]) 50 U.S.C. § 1803 (i)(2)(A).

([265]) 50 U.S.C. § 1803 (i)(2)(B).

([266]) Ver, por exemplo, o parecer do FISC de 18 de outubro de 2018, disponível em athttps:// www.intelligence.gov/assets/documents/ /702%20Documents/declassified/2018_Cert_FISC_Opin_18Oct18.pdf, tal como confirmado pelo *Foreign Intelligence Court of Review* no seu parecer de 12 de julho de 2019, disponível em athttps:// www.intelligence.gov/assets/documents/702%20Documents/ /declassified/2018_Cert_FISCR_Opinion_12Jul19.pdf.

([267]) Ver, por exemplo, FISC, *Memorandum Opinion and Order at 35* (18 de novembro de 2020) (autorizado para divulgação pública em 26 de abril de 2021) (anexo D).

([268]) 50 U.S.C. § 1881a(a), *Procedures used by the National Security Agency for Targeting Non-United States Persons Reasonably Believed to be Located outside the United States to Acquire Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978*, alterado, de março de 2018 (*NSA targeting procedures*), disponível em: athttps://www.intelligence.gov/assets/documents/ /702%20Documents/declassified/2018_Cert_NSA_Targeting_27Mar18.pdf, p. 1-4, explicado mais circunstanciadamente no relatório da PCLOB, p. 41-42.

um juízo analítico, pela formação especializada e pela experiência do analista, bem como pela natureza das informações externas a obter ([269]). A seleção de alvos é efetuada através da identificação dos chamados «seletores» que identificam meios de comunicação específicos, como o endereço de correio eletrónico ou o número de telefone do cidadão visado, mas nunca palavras-chave nem os nomes dos cidadãos ([270]).

(146) Os analistas da NSA identificarão, em primeiro lugar, os cidadãos de países terceiros localizados no estrangeiro cuja vigilância conduzirá, com base na avaliação do analista, às informações externas pertinentes especificadas na certificação ([271]). Tal como estabelecido nos procedimentos de seleção de alvos da NSA, a NSA só pode orientar a vigilância para um alvo quando já tiver conhecimento de algo sobre o alvo ([272]). Este conhecimento pode resultar de informações provenientes de diferentes fontes, por exemplo, de informações humanas. Através destas outras fontes, o analista deve também conhecer um seletor específico (ou seja, uma conta de comunicação) utilizado pelo potencial alvo. Após a identificação destas pessoas e a sua aprovação como objetivos por um amplo mecanismo de análise no âmbito da NSA ([273]), 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 ([274]).

(147) A NSA deve documentar a fundamentação factual para a seleção do alvo ([275]) e, a intervalos regulares após a seleção inicial do alvo, confirmar que a norma de seleção de alvos continua a ser cumprida ([276]). Se a norma de seleção de alvos deixar de ser cumprida, a recolha deve ser interrompida ([277]). Os funcionários dos gabinetes de supervisão dos serviços de informações do *Department of Justice*, que têm a obrigação de comunicar qualquer violação ao FISC e ao Congresso, analisam, de dois em dois meses, a seleção de cada alvo pela NSA e o respetivo registo de avaliação e fundamentação da seleção do alvo para verificar o cumprimento com os procedimentos de seleção de alvos ([278]). A documentação escrita da NSA facilita a supervisão do FISC sobre se determinados cidadãos são devidamente visados nos termos da secção 702 da FISA, de acordo com os seus poderes de supervisão descritos nos considerandos 173 a 174 ([279]). Por último, o *Director of National Intelligence* deve também comunicar todos os anos o número total de alvos nos termos da secção 702 da FISA nos relatórios anuais públicos de transparência estatística. As empresas que recebem diretivas nos termos da secção 702 da FISA podem publicar dados agregados (através de relatórios de transparência) relativos aos pedidos que recebem ([280]).

([269]) *NSA targeting procedures*, p. 4.

([270]) PCLOB, Sec. 702 Report, p. 32-33 e 45 com referências adicionais. Ver também a *Semiannual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* apresentada pelo *Attorney General* e pelo *Director of National Intelligence*, período de referência: de 1 de dezembro de 2016 a 31 de maio de 2017, p. 41 (outubro de 2018), disponível em: https://www.dni.gov/files/icotr/18th_Joint_Assessment.pdf.

([271]) PCLOB, Sec. 702 Report, p. 42-43.

([272]) *NSA targeting procedures*, p. 2.

([273]) PCLOB, Sec. 702 Report, p. 46. Por exemplo, a NSA deve verificar se existe uma relação entre o alvo e o seletor, deve documentar no estrangeiro as informações que prevê obter, estas informações devem ser analisadas 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, 16.4.2014.

([274]) 50 U.S.C. § 1881a (h).

([275]) *NSA targeting procedures*, p. 8. Ver também PCLOB, *Section 702 Report*, p. 46. A não apresentação de uma justificação escrita constitui uma situação de não conformidade da documentação, que deve ser comunicada ao FISC e ao Congresso. Ver a *Semiannual Assessment of Compliance with Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* apresentada pelo *Attorney General* e pelo *Director of National Intelligence*, período de referência: de 1 de dezembro de 2016 a 31 de maio de 2017, p. 41 (outubro de 2018), Relatório de conformidade do DOJ/ODNI ao FISC para o período de dezembro de 2016 a maio de 2017, p. A-6, disponível em: https://www.dni.gov/files/icotr/18th_Joint_Assessment.pdf.

([276]) Ver a petição do Governo dos EUA ao *Foreign Intelligence Surveillance Court*, *2015 Summary of Notable Section 702 Requirements*, p. 2 a 3 (15 de julho de 2015), e as informações constantes do anexo VII.

([277]) Ver a petição do Governo dos EUA ao *Foreign Intelligence Surveillance Court*, *2015 Summary of Notable Section 702 Requirements*, p. 2 a 3 (15 de julho de 2015), que prevê que «[s]e o governo avaliar posteriormente que não se espera que a continuação da tarefa do seletor de um alvo conduza à obtenção de informações externas, esta deve ser interrompida de imediato, sendo que o adiamento pode resultar numa situação de incumprimento comunicável». Ver também as informações constantes do anexo VII.

([278]) PCLOB, Sec. 702 Report, p. 70-72. Regra 13, alínea b), do regulamento interno do *Intelligence Surveillance Court* dos Estados Unidos, disponível em: https://www.fisc.uscourts.gov/sites/default/files/FISC%20Rules%20of%20Procedure.pdf.

([279]) Ver também o Relatório de conformidade do DOJ/ODNI ao FISC para o período de dezembro de 2016 a maio de 2017, p. A-6.

([280]) 50 U.S.C. § 1874.

(148) No que diz respeito às outras bases jurídicas para a recolha de dados pessoais transferidos para organizações localizadas nos EUA, aplicam-se limitações e garantias diferentes. Em geral, a recolha de dados em larga escala é especificamente proibida nos termos da secção 402 da FISA (autoridade em matéria de dispositivos de registo de chamadas telefónicas e comunicações eletrónicas) e através da utilização de NSL, sendo, ao invés, exigida a utilização de «termos de seleção» específicos ([281]).

(149) Para realizar uma vigilância eletrónica individualizada convencional (nos termos da secção 105 da FISA), os serviços de informações devem apresentar um pedido ao FISC em que conste uma declaração dos factos e circunstâncias subjacentes para justificar a convicção de que existe uma causa provável de que a instalação é utilizada, ou está prestes a ser utilizada, por uma potência estrangeira ou por um agente de uma potência estrangeira ([282]). O FISC avaliará, entre outros aspetos, se, com base nos factos apresentados, existe uma causa provável de que tal se verifica efetivamente ([283]).

(150) Para efetuar uma busca de instalações ou bens que se destine a resultar numa inspeção, apreensão, etc. de informações, material ou bens (por exemplo, um dispositivo informatizado) com base na secção 301 da FISA, é necessário obter uma decisão do FISC ([284]). Esse pedido deve, nomeadamente, demonstrar que existe uma causa provável de que o alvo da busca é uma potência estrangeira ou um agente de uma potência estrangeira, que a instalação ou os bens objeto da busca contêm informações externas e que a instalação objeto da busca é propriedade, utilizada, detida ou está a ser transferida de um (agente de uma) potência estrangeira ou para um (agente de uma) potência estrangeira ([285]).

(151) Do mesmo modo, a instalação de dispositivos de registo de chamadas telefónicas e comunicações eletrónicas (nos termos da secção 402 da FISA) implica um pedido de decisão do FISC (ou de um magistrado norte-americano) e a utilização de um termo de seleção específico, ou seja, um termo que identifique especificamente um cidadão, uma conta, etc., e que seja utilizado para limitar, tanto quanto razoavelmente possível, o âmbito das informações solicitadas ([286]). Esta faculdade 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).

(152) A secção 501 da FISA ([287]), que permite a recolha de documentação empresarial de uma empresa de transportes públicos (ou seja, qualquer cidadão ou entidade que transporte pessoas ou bens por via terrestre, ferroviária, marítima ou aérea mediante remuneração), de uma unidade de alojamento pública (por exemplo, um hotel, motel ou estalagem), de um estabelecimento de aluguer de veículos ou de um estabelecimento de armazenamento físico (ou seja, que forneça espaço ou preste serviços relacionados com o armazenamento de mercadorias e materiais) ([288]), também exige um pedido ao FISC ou a um magistrado. Este pedido deve especificar a documentação solicitada e os factos específicos e articuláveis que justificam a convicção de que o cidadão a quem a documentação diz respeito é uma potência estrangeira ou um agente de uma potência estrangeira ([289]).

(153) Por último, diferentes leis autorizam a utilização de NSL. Além disso, as NSL permitem que as agências de investigação obtenham certas informações (não incluindo o conteúdo das comunicações) de determinadas entidades (por exemplo, instituições financeiras, agências de informações comerciais, prestadores de serviços de comunicações eletrónicas) constantes de relatórios de crédito, registos financeiros e registos eletrónicos de assinantes e transnacionais ([290]). A lei relativa às NSL que autoriza o acesso às comunicações eletrónicas só pode ser utilizada pelo FBI e exige que os pedidos utilizem um termo que identifique especificamente um cidadão, entidade, número de telefone ou conta e que certifique que as informações são pertinentes para uma investigação de segurança nacional autorizada com vista à proteção contra o terrorismo internacional ou atividades de informações clandestinas ([291]). Os destinatários de uma NSL têm o direito de a impugnar em tribunal ([292]).

([281]) 50 U.S. Code § 1842(c)(3) e, no que respeita às NSL, 12 U.S.C. § 3414(a)(2); 15 U.S.C. § 1681u; 15 U.S.C. § 1681v(a); e 18 U.S.C. § 2709(a).

([282]) Um «agente de uma potência estrangeira» 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)].

([283]) 50 U.S.C. § 1804. Ver também § 1841(4) no que diz respeito à escolha dos termos de seleção.

([284]) 50 U.S.C. § 1821(5).

([285]) 50 U.S.C. § 1823(a).

([286]) 50 U.S.C. § 1842 com § 1841(2) e secção 3127 do título 18.

([287]) 50 U.S.C. § 1862.

([288]) 50 U.S.C. §§ 1861-1862.

([289]) 50 U.S.C. § 1862 (b).

([290]) 12 U.S.C. § 3414; 15 U.S.C. §§ 1681u-1681v; e 18 U.S.C. § 2709.

([291]) 18 U.S.C. § 2709 (b).

([292]) Por exemplo, 18 U.S.C. § 2709(d).

3.2.1.3 *Utilização adicional das informações recolhidas*

(154) O tratamento de dados pessoais recolhidos pelos serviços de informações dos EUA através de informação de origem eletromagnética está sujeito a uma série de garantias.

(155) Em primeiro lugar, cada serviço de informações deve assegurar a segurança adequada dos dados e impedir o acesso de cidadãos não autorizados aos dados pessoais recolhidos através de informação de origem eletromagnética. A este respeito, diferentes instrumentos, nomeadamente leis, orientações e normas, especificam os requisitos mínimos de segurança da informação que têm de ser aplicados (por exemplo, autenticação multifatores, cifragem, etc.) ([293]). O acesso aos dados recolhidos deve ser limitado ao pessoal autorizado e qualificado com necessidade de conhecer as informações para desempenhar a sua missão ([294]). Em termos mais gerais, os serviços de informações devem ministrar formação adequada aos seus trabalhadores, nomeadamente sobre os procedimentos de comunicação e tratamento das violações da lei (incluindo o EO 14086) ([295]).

(156) Em segundo lugar, os serviços de informações devem cumprir as normas do setor das informações em matéria de exatidão e objetividade, em especial no que diz respeito à garantia da qualidade e fiabilidade dos dados, à consideração de fontes alternativas de informação e à objetividade na realização de análises ([296]).

(157) Em terceiro lugar, no que respeita à conservação de dados, o EO 14086 esclarece que os dados pessoais de cidadãos de países terceiros estão sujeitos aos mesmos períodos de conservação que os aplicáveis aos dados de cidadãos norte-americanos ([297]). Os serviços de informações são obrigados a definir períodos de conservação específicos e/ou os fatores que devem ser tidos em conta para determinar a duração dos períodos de conservação aplicáveis (por exemplo, se a informação constitui prova de um crime; se os dados constituem dados de informações estrangeiras; se as informações são necessárias para proteger a segurança de pessoas ou organizações, incluindo vítimas ou alvos de terrorismo internacional), que estão definidos em diferentes instrumentos jurídicos ([298]).

(158) Em quarto lugar, aplicam-se regras específicas no que respeita à divulgação de dados pessoais recolhidos através de informação de origem eletromagnética. Como requisito geral, os dados pessoais relativos a cidadãos de países terceiros só podem ser divulgados se envolverem o mesmo tipo de informações autorizadas a ser divulgadas sobre cidadãos norte-americanos, por exemplo, informações necessárias para proteger a segurança de um cidadão ou organização (como alvos, vítimas ou reféns de organizações terroristas internacionais) ([299]). Além disso, os dados pessoais não podem ser divulgados exclusivamente devido à nacionalidade ou ao país de residência de um cidadão ou com o objetivo de contornar os requisitos constantes do EO 14086 ([300]). A divulgação no seio do Governo dos EUA só pode ter lugar se uma pessoa autorizada e qualificada tiver uma convicção razoável de que o destinatário

([293]) Secção 2(c)(iii)(B)(1) do EO 14086. Ver também o título VIII da *National Security Act* (que especifica os requisitos de acesso às informações classificadas), a secção 1.5 do EO 12333 (que exige que os diretores das agências do setor das informações respeitem as orientações sobre partilha e segurança da informação, proteção da privacidade da informação e outros requisitos legais), a *National Security Directive 42* intitulada «National Policy for the Security of National Security Telecommunications and Information Systems» (que dá instruções ao *Committee on National Security Systems* para fornecer aos departamentos e agências executivos orientações sobre a segurança dos sistemas de segurança nacional) e o *National Security Memorandum 8* intitulado «Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems» (que estabelece prazos e orientações sobre a forma como os requisitos de cibersegurança serão aplicados aos sistemas de segurança nacional, nomeadamente a autenticação multifatores, a cifragem, as tecnologias de computação em nuvem e os serviços de deteção de pontos finais).

([294]) Secção 2(c)(iii)(B)(2) do EO 14086. Além disso, os dados pessoais para os quais não tenha sido tomada uma decisão final de conservação só podem ser acedidos para tomar ou apoiar essa decisão ou para o exercício de funções administrativas, de ensaio, de desenvolvimento, de segurança ou de supervisão autorizadas [secção 2(c)(iii)(B)(3) do EO 14086].

([295]) Secção 2(d)(ii) do EO 14086.

([296]) Secção 2(c)(iii)(C) do EO 14086.

([297]) Secção 2(c)(iii)(A)(2)(a)-(c) do EO 14086. Em termos mais gerais, cada serviço deve pôr em prática políticas e procedimentos destinados a minimizar a divulgação e a conservação de dados pessoais recolhidos através de informação de origem eletromagnética [secção 2(c)(iii)(A) do EO 14086].

([298]) Ver, por exemplo, Secção 309 da *Intelligence Authorization Act for Fiscal Year 2015*. procedimentos de minimização adotados por serviços de informações individuais ao abrigo da secção 702 da FISA e autorizados pelo FISC; procedimentos aprovados pelo *Attorney General* e pela FRA (impondo às agências federais dos EUA, incluindo as agências nacionais de segurança, a definição de períodos de conservação dos seus registos que devem ser aprovados pela *National Archives and Record Administration*).

([299]) Secção 2(c)(iii)(A)(1)(a) e 5(d) do EO 14086 em conjugação com a secção 2.3 do EO 12333.

([300]) Secção 2(c)(iii)(A)(1)(b) e (e) do EO 14086.

tem necessidade de conhecer as informações ([301]) e que as protegerá de modo adequado ([302]). Para determinar se os dados pessoais podem ser divulgados a destinatários fora do Governo dos EUA (nomeadamente um governo estrangeiro ou uma organização internacional), há que ter em conta a finalidade da divulgação, a natureza e o volume dos dados divulgados e o potencial impacto negativo no(s) cidadão(s) em causa ([303]).

(159) Por último, nomeadamente para facilitar a supervisão do cumprimento dos requisitos legais aplicáveis, bem como mecanismos de recurso eficazes, cada serviço de informações é obrigado, nos termos do EO 14086, a conservar documentação adequada sobre a recolha de informação de origem eletromagnética. Os requisitos relativos à documentação abrangem elementos como a base factual para a avaliação da necessidade de realizar uma atividade de recolha específica com vista a promover uma prioridade em matéria de informações validada ([304]).

(160) Para além das salvaguardas acima referidas ao abrigo do EO 14086 para a utilização de informações recolhidas através de informações de origem eletromagnética, todos os serviços de informações dos EUA estão sujeitos a requisitos mais gerais em matéria de limitação da finalidade, minimização dos dados, exatidão, segurança, conservação e divulgação, em especial nos termos da Circular n.º A-130 da OMB, da *E-Government Act*, da *Federal Records Act* (ver considerandos101-106) e das orientações do *Committee on National Security Systems* (CNSS) ([305]).

3.2.2. ***Supervisão***

(161) As atividades dos serviços de informações dos EUA estão sujeitas à supervisão de diferentes organismos.

(162) Em primeiro lugar, o EO 14086 exige que cada serviço de informações tenha funcionários a nível superior com experiência nos domínios jurídico, da supervisão e da conformidade para assegurar o cumprimento da legislação dos EUA aplicável ([306]). Em especial, os referidos funcionários devem efetuar uma supervisão periódica das atividades de informação de origem eletromagnética e assegurar a correção de qualquer incumprimento identificado. Os serviços de informações devem fornecer a esses funcionários acesso a todas as informações relevantes para o exercício das suas funções de supervisão e não podem tomar quaisquer medidas para impedir ou influenciar indevidamente as suas atividades de supervisão ([307]). Além disso, qualquer situação de incumprimento grave ([308]) identificado por um funcionário de supervisão ou por qualquer outro funcionário deve ser prontamente comunicado ao diretor do serviço de informações e ao *Director of National Intelligence*, que devem assegurar que são adotadas todas as medidas necessárias para corrigir e evitar a recorrência da situação de incumprimento grave ([309]).

(163) Esta função de supervisão é desempenhada por agentes com uma função de verificação da conformidade designada, bem como por agentes responsáveis pela proteção da privacidade e das liberdades cívicas e por inspetores-gerais ([310]).

([301]) O AGG-DOM, por exemplo, estabelece que o FBI só pode divulgar informações se o destinatário tiver necessidade de saber para cumprir a sua missão ou para proteger o público.

([302]) Secção 2(c)(iii)(A)(1)(c) do EO 14086. Os serviços de informações podem, por exemplo, divulgar informações em circunstâncias pertinentes para uma investigação criminal ou relacionadas com um crime, nomeadamente através da divulgação de alertas de ameaças de morte, lesões corporais graves ou raptos; divulgar informações relativas às ciberameaças e à resposta a intrusões e incidentes informáticos; e notificar as vítimas ou alertar potenciais vítimas de crimes.

([303]) Secção 2(c)(iii)(A)(1)(d) do EO 14086.

([304]) Secção 2(c)(iii)(E) do EO 14086.

([305]) Ver *Cybersecurity Risk Management Policy* e a *Instruction 1253* do CNSS, que fornecem orientações pormenorizadas sobre as medidas de segurança a adotar para os sistemas de segurança nacionais.

([306]) Secção 2(d)(i)(A)-(B) do EO 14086.

([307]) Secção 2(d)(i)(B)-(C) do EO 14086.

([308]) Ou seja, um incumprimento sistémico ou intencional da legislação dos EUA aplicável, suscetível de comprometer a reputação ou a integridade de um elemento do setor das informações ou, de outro modo, pôr em causa a idoneidade de uma atividade do setor das informações, incluindo tendo em conta qualquer impacto significativo nos interesses da privacidade e das liberdades cívicas do cidadão ou cidadãos em causa. Ver secção 5(l) do EO 14086.

([309]) Secção 2(d)(iii) do EO 14086.

([310]) Secção 2(d)(i)(B) do EO 14086.

(164) Tal como acontece com as autoridades responsáveis pela aplicação do direito penal, em todos os serviços de informações existem agentes responsáveis pela proteção da privacidade e das liberdades cívicas ([311]). Os poderes específicos destes agentes, habitualmente 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 dos cidadãos que consideram que a sua privacidade ou liberdades cívicas foram violadas (e, em alguns casos, como o *Office of the Director of National Intelligence* (ODNI), podem ter competência para investigar queixas ([312])). Os diretores dos serviços de informações devem assegurar que os agentes responsáveis pela proteção da privacidade e das liberdades cívicas dispõem dos recursos necessários para cumprir o seu mandato, têm acesso a todo o material e pessoal necessário para o exercício das suas funções e são informados e consultados sobre as alterações políticas propostas ([313]). 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 dessas queixas, as análises efetuadas e as questões colocadas e ainda o impacto das atividades levadas a cabo pelo agente ([314]).

(165) Em segundo lugar, cada serviço de informações tem um inspetor-geral independente que, entre outras funções, é responsável pela supervisão das atividades de informações externas. Isto inclui, no âmbito do ODNI, um *Office of the Inspector General* (gabinete do inspetor-geral) do setor das informações com competência abrangente sobre todo este, que tem autorização para 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 ([315]). À semelhança do que se verifica no caso das autoridades responsáveis pela aplicação do direito penal (ver considerando 109), esses inspetores-gerais são juridicamente independentes ([316]) e responsáveis pela realização de auditorias e investigações relacionadas com os programas e operações levados a cabo pelo respetivo serviço para efeitos de prestações de informações nacionais, nomeadamente no que diz respeito a abusos ou violações da lei ([317]). Podem aceder a todos os registos, relatórios, auditorias, revisões, documentos, recomendações ou outros materiais pertinentes, através de

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

([312]) Ver secção 3(c) do EO 14086.

([313]) 42 U.S.C. § 2000ee-1(d).

([314]) See 42 U.S.C. § 2000ee-1 (f)(1),(2). Por exemplo, o relatório do *Civil Liberties, Privacy and Transparency Office* da NSA, relativo ao período compreendido entre janeiro de 2021 e junho de 2021, mostra que o gabinete realizou 591 análises dos impactos nas liberdades cívicas e na privacidade em vários contextos, por exemplo, no que diz respeito a atividades de recolha, a acordos e decisões de partilha de informações, a decisões de conservação de dados, etc., tendo em conta diferentes fatores, como a quantidade e o tipo de informações associadas à atividade, os cidadãos envolvidos, a finalidade e a utilização prevista dos dados, as garantias em vigor para atenuar os potenciais riscos para a privacidade, etc. (https://media.defense.gov/2022/Apr/11/2002974486/-1/-1/1/ /REPORT%207_CLPT%20JANUARY%20-%20JUNE%202021%20_FINAL.PDF). Do mesmo modo, os relatórios do *Office of Privacy and Civil Liberties* da CIA relativos ao período compreendido entre janeiro e junho de 2019 fornecem informações sobre as atividades de supervisão do gabinete, por exemplo, uma análise do cumprimento das orientações do *Attorney General* nos termos do EO 12333 no que diz respeito à conservação e divulgação de informações, às orientações fornecidas sobre a aplicação da PPD 28 e aos requisitos para identificar e resolver violações de dados, bem como análises da utilização e tratamento de informações pessoais (https://www.cia.gov/static/9d762fbef6669c7e6d7f17e227fad82c/2019-Q1-Q2-CIA-OPCL-Semi-Annual-Report.pdf).

([315]) Este inspetor-geral é nomeado pelo presidente, com a confirmação do Senado, e só pode ser destituído pelo presidente.

([316]) O cargo dos 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 faculdade 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 (para o DOJ), § 8G (d)(2)(A),(B) (para a NSA); 50. U.S.C. § 403q b) (IG da CIA); *Intelligence Authorization Act For Fiscal Year 2010*, Sec. 405f) (do setor das informações).

([317]) Ver também a *Inspector General Act* de 1978, alterada, Pub. L. 117-108 de 8 de abril de 2022. Por exemplo, conforme explicado nos seus relatórios semestrais ao Congresso relativos ao período compreendido entre 1 de abril de 2021 e 31 de março de 2022, o inspetor-geral da NSA realizou avaliações do tratamento de informações sobre cidadãos norte-americanos recolhidas nos termos do EO 12333, do processo de eliminação de informação de origem eletromagnética, de uma ferramenta automatizada de seleção de alvos utilizada pela NSA e do cumprimento das regras em matéria de documentação e consulta no que diz respeito à recolha prevista na secção 702 da FISA, tendo emitido várias recomendações neste contexto (ver https://oig.nsa.gov/Portals/71/Reports/SAR/NSA%20OIG%20SAR%20-%20APR%202021%20-%20SEP%202021%20-%20Unclassified.pdf?ver=IwtrthntGdfEb-EKTOm3gg%3d%3d, p. 5-8 e https://oig.nsa.gov/Portals/71/Images/NSAOIGMAR2022.pdf?ver=jbq2rCrJ00HJ9qDXGHqHLw%3d%3d&timestamp=1657810395907, p. 10-13). Ver também as recentes auditorias e investigações levadas a cabo pelo inspetor-geral do setor das informações sobre a segurança da informação e a divulgação não autorizada de informações de segurança nacional classificadas (https://www.dni.gov/files/ICIG/Documents/Publications/Semiannual%20Report/2021/ICIG_Semiannual_Report_April_2021_to_September_2021.pdf, p. 8 e 11, e https://www.dni.gov/files/ICIG/Documents/News/ICIGNews/2022/Oct21_SAR/Oct%202021-Mar%202022%20ICIG%20SAR_Unclass_FINAL.pdf, p. 19-20).

intimações, se necessário, e podem recolher depoimentos ([318]). Os inspetores-gerais remetem os casos de suspeita de infrações penais para os tribunais para o exercício da ação penal e formulam recomendações sobre medidas corretivas destinadas aos diretores dos serviços ([319]). Embora as suas recomendações não sejam vinculativas, os seus relatórios, incluindo as medidas de acompanhamento (ou a sua inexistência) ([320]), são geralmente tornados públicos e transmitidos ao Congresso, que pode, com base neles, exercer a sua própria função de supervisão (ver considerandos 168 e 169) ([321]).

(166) Em terceiro lugar, o *Intelligence Oversight Board* (IOB), criado no âmbito do *President's Intelligence Advisory Board* (PIAB), supervisiona o cumprimento da Constituição e de todas as regras aplicáveis por parte dos serviços de informações dos EUA ([322]). O PIAB é um órgão consultivo do *Executive Office of the President* constituído por 16 membros fora do Governo dos EUA nomeados pelo presidente. O IOB é constituído por um máximo de cinco membros designados pelo presidente de entre os membros do PIAB. Em conformidade com o EO 12333 ([323]), os diretores de todos os serviços de informações são obrigados a comunicar ao IOB qualquer atividade de informações relativamente à qual existam razões para crer que possa ser ilegal ou contrária a um decreto executivo ou diretiva presidencial. Para assegurar que o IOB tem acesso às informações necessárias para o exercício das suas funções, o EO 13462 dá instruções ao *Director of National Intelligence* e aos diretores dos serviços de informações para que prestem quaisquer informações e assistência que o IOB determine serem necessárias para o exercício das suas funções, na medida do permitido pela lei ([324]). Por sua vez, o IOB é obrigado a informar o presidente sobre atividades de informações que considera poderem estar a violar a legislação dos EUA (incluindo decretos executivos) e que não estejam a ser adequadamente tratadas pelo *Attorney General*, pelo *Director of National Intelligence* ou pelo diretor de um serviço de informações ([325]). Além disso, o IOB é obrigado a informar o *Attorney General* sobre eventuais violações do direito penal.

(167) Em quarto lugar, os serviços de informações estão sujeitos à supervisão da PCLOB. De acordo com o seu estatuto constitutivo, a PCLOB tem responsabilidades no domínio das políticas de luta contra o terrorismo e da sua aplicação, com vista à proteção da privacidade e das liberdades cívicas. Na sua análise das ações dos serviços de informações, pode aceder a todos os registos, relatórios, auditorias, análises, documentos e recomendações dos serviços de informações pertinentes, nomeadamente informações classificadas, realizar entrevistas e recolher depoimentos ([326]). Recebe relatórios dos agentes responsáveis pela proteção da privacidade e das liberdades cívicas de vários departamentos/serviços federais ([327]), pode emitir recomendações às autoridades governamentais e às agências de informação, e informa regularmente os comités do Congresso e ao Presidente ([328]). Os relatórios do conselho, incluindo os que são apresentados ao Congresso, devem ser, na medida do possível, disponibilizados ao público ([329]). A PCLOB emitiu vários relatórios de supervisão e acompanhamento, incluindo uma análise dos programas executados com base na secção 702 da FISA e a proteção da privacidade neste contexto, a aplicação da PPD 28 e do EO 12333 ([330]). Cabe também à PCLOB exercer funções de supervisão específicas no que se refere à

([318]) Ver a *Inspector General Act* de 1978, § 6.

([319]) Ver ibid. §§ 4, 6-5.

([320]) No que diz respeito ao seguimento dado aos relatórios e às recomendações dos inspetores-gerais, ver, por exemplo, a resposta a um relatório do inspetor-geral do DOJ que concluiu que o FBI não foi suficientemente transparente com o FISC nos pedidos apresentados entre 2014 e 2019, o que conduziu a reformas para melhorar o cumprimento, a supervisão e a responsabilização no FBI (por exemplo, o diretor do FBI decretou mais de 40 medidas corretivas, incluindo 12 específicas do processo FISA relacionadas com documentação, supervisão, manutenção de ficheiros, formação e auditorias) (ver https://www.justice.gov/opa/pr/department-justice-and-federal-bureau-investigation-announce-critical-reforms-enhance e https://oig.justice.gov/reports/2019/o20012.pdf). Ver também, por exemplo, a auditoria do inspetor-geral do DOJ sobre as funções e responsabilidades do *Office of the General Counsel* do FBI na supervisão do cumprimento da legislação, políticas e procedimentos aplicáveis relacionados com as atividades de segurança nacional do FBI e o apêndice 2, que inclui uma carta do FBI em que este aceita todas as recomendações. A este respeito, o apêndice 3 apresenta uma panorâmica das medidas de acompanhamento e das informações que o inspetor-geral solicitou ao FBI para poder concluir as suas recomendações (https://oig.justice.gov/sites/default/files/reports/22-116.pdf).

([321]) Ver a *Inspector General Act* de 1978, §§ 4(5), 5.

([322]) Ver EO 13462.

([323]) Secção 1.6(c) do EO 12333.

([324]) Secção 8(a) do EO 13462.

([325]) Secção 6(b) do EO 13462.

([326]) 42 U.S.C. § 2000ee g).

([327]) Ver 42 U.S.C. § 2000ee-1 (f)(1)(A)(iii). 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 que a PCLOB considere pertinente.

([328]) 42 U.S.C. §2000ee (e).

([329]) 42 U.S.C. § 2000ee (f).

([330]) Disponível em https://www.pclob.gov/Oversight.

aplicação do EO 14086, em especial verificando se os procedimentos das agências são coerentes com o decreto executivo (ver considerando 126) e avaliando a correção do funcionamento do mecanismo de recurso (ver considerando 194).

(168) Em quinto lugar, para além dos mecanismos de supervisão no quadro do poder executivo, existem comités específicos no Congresso dos EUA (os *House and Senate Intelligence and Judiciary Committees*) que têm responsabilidades de supervisão relativamente a todas as atividades de informações externas dos EUA. Os membros destes comités têm acesso a informações classificadas, bem como a métodos e programas de informações ([331]). Os comités exercem as suas funções de supervisão de diferentes formas, nomeadamente através de audições, investigações, análises e relatórios ([332]).

(169) Os comités do Congresso recebem relatórios regulares sobre as atividades de informações, nomeadamente do *Attorney General*, do *Director of National Intelligence*, dos serviços de informações e de outros organismos de supervisão (por exemplo, inspetores-gerais). Ver considerandos 164 e 165. Em particular, 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». ([333]) Além disso, «[o] Presidente deve assegurar que todas as atividades de informação 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». ([334])

(170) Além disso, requisitos de comunicação adicionais decorrem de leis específicas. Em especial, 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 ([335]). Exige ainda que o governo apresente aos comités do Congresso cópias de todas as decisões, despachos ou pareceres do FISC ou do FISCR que incluam construção ou interpretação significativas das disposições da FISA. No que se refere à vigilância nos termos da secção 702 da FISA, a supervisão parlamentar 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, nomeadamente os relatórios de conformidade do *Department of Justice* e do ODNI, bem como uma descrição de todas as situações de incumprimento ([336]), e uma avaliação semestral separada efetuada pelo *Attorney General* e pelo *Director of National Intelligence* que documenta a conformidade com os procedimentos de orientação e minimização ([337]).

([331]) 50 U.S.C. § 3091.

([332]) Por exemplo, os comités organizam audições temáticas (ver, a título de exemplo, uma audição recente do *House Judiciary Committee* sobre «redes de arrasto digitais», https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4983 e uma audição do *House Intelligence Committee*sobre a utilização da IA pelo setor das informações, https://docs.house.gov/Committee/Calendar/ByEvent.aspx?EventID=114263), e audições regulares de supervisão, por exemplo, do FBI e da *National Security Division* do DOJ, ver https://www.judiciary.senate.gov/meetings/08/04/2022/oversight-of-the-federal-bureau-of-investigation; https://judiciary.house.gov/calendar//eventsingle.aspx?EventID=4966 e https://judiciary.house.gov/calendar/eventsingle.aspx?EventID=4899. A título de exemplo de uma investigação, ver a investigação do *Senate Intelligence Committee* sobre a interferência russa nas eleições norte-americanas de 2016, em https://www.intelligence.senate.gov/publications/report-select-committee-intelligence-united-states-senate-russian-active-measures.
Em termos de relatórios, ver, por exemplo, o resumo das atividades (supervisão) do comité constante do relatório do *Senate Intelligence Committee* relativo ao período compreendido entre 4 de janeiro de 2019 e 3 de janeiro de 2021 ao Senado, https://www.intelligence.senate.gov/publications/report-select-committee-intelligence-united-states-senate-covering-period-january-4.

([333]) Ver 50 U.S.C. § 3091(a)(1). Esta disposição contém os requisitos gerais no que se refere à supervisão efetuada pelo Congresso no domínio da segurança nacional.

([334]) Ver 50 U.S.C. §3091(b).

([335]) See 50 U.S.C. §§ 1808, 1846, 1862, 1871, 1881f.

([336]) See 50 U.S.C. § 1881f.

([337]) See 50 U.S.C. § 1881a(l)(1).

(171) Além disso, a FISA determina que o governo dos EUA divulgue anualmente ao Congresso (e ao público) o número de decisões solicitadas e recebidas nos termos da FISA, bem como as estimativas do número de cidadãos norte-americanos e de países terceiros que são alvo de vigilância, entre outros ([338]). A referida lei exige igualmente a comunicação pública adicional do número de NSL emitidas, novamente no que 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) ([339]).

(172) Em termos mais gerais, o setor de informações norte-americano envida vários esforços para proporcionar transparência sobre as suas atividades de informações (externas). Por exemplo, em 2015, o ODNI adotou os princípios de transparência de informações e um plano de aplicação da transparência e deu instruções a cada serviço de informações para designar um *Intelligence Transparency Officer* para promover a transparência e liderar iniciativas de transparência ([340]). No âmbito destes esforços, o setor das informações tornou e continua a tornar públicas partes desclassificadas de políticas, procedimentos, relatórios de supervisão, relatórios sobre atividades nos termos da secção 702 da FISA e do EO 12333, decisões do FISC e outros materiais, nomeadamente numa página Web específica, *IC on the Record*, gerida pelo ODNI ([341]).

(173) Por último, a recolha de dados pessoais nos termos da secção 702 da FISA está sujeita, para além da supervisão pelos organismos de supervisão referidos nos considerandos 162 a 168, à supervisão do FISC ([342]). Nos termos da regra 13 do regulamento interno do FISC, os responsáveis pela conformidade dos serviços de informações dos EUA são obrigados a comunicar quaisquer violações dos procedimentos de orientação, minimização e consulta previstos na secção 702 da FISA ao DOJ e ao ODNI, que, por sua vez, as comunicam ao FISC. Além disso, o DOJ e o ODNI apresentam ao FISC relatórios semestrais de avaliação da supervisão conjunta, que identificam as tendências de cumprimento da seleção de alvos, fornecem dados estatísticos, descrevem categorias de situações de incumprimento, descrevem em pormenor os motivos segundo os quais ocorreram determinadas situações de incumprimento da seleção de alvos e descrevem as medidas que os serviços de informações tomaram para evitar que se repitam ([343]).

(174) Sempre que necessário (por exemplo, se forem identificadas violações dos procedimentos de seleção de alvos), o Tribunal pode ordenar ao serviço de informações competente que tome medidas corretivas ([344]). As medidas corretivas em causa podem ir desde medidas individuais a medidas estruturais, por exemplo, da cessação da recolha de dados e a eliminação de dados obtidos ilegalmente à alteração das práticas de recolha, incluindo as orientações e a formação do pessoal ([345]). Além disso, durante a sua análise anual das certificações previstas na secção 702, o FISC tem em conta situações de incumprimento para determinar se as certificações apresentadas cumprem os requisitos

([338]) 50 U.S.C. § 1873 (b). Além disso, segundo a secção 402, «o *Director of National Intelligence*, em consulta com o *Attorney General*, deve levar a cabo uma reapreciação de desclassificação de cada decisão ou parecer emitido pelo *Foreign Intelligence Surveillance Court* ou o *Foreign Intelligence Surveillance Court of Review* [tribunal competente para apreciar os recursos relativos aos pedidos e mandatos em matéria de vigilância — conforme estabelecido na secção 601(e)], que inclua uma interpretação ou explicação significativa de qualquer disposição da legislação, incluindo qualquer interpretação ou explicação 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.

([339]) 50 U.S.C. §§ 1873(b)(7) e 1874.

([340]) https://www.dni.gov/index.php/ic-legal-reference-book/the-principles-of-intelligence-transparency-for-the-ic.

([341]) Ver *IC on the Record*, disponível em: https://icontherecord.tumblr.com/.

([342]) No passado, o FISC concluiu que «[é] evidente para o Tribunal que as agências de execução, bem como o [ODNI] e a [*National Security Division* do DOJ], afetem recursos significativos às suas responsabilidades de conformidade e supervisão nos termos da secção 702. Regra geral, as situações de incumprimento são identificadas de imediato e adotadas medidas corretivas adequadas, em especial a eliminação de informações obtidas indevidamente ou de outro modo sujeitas aos requisitos em matéria de destruição no âmbito dos procedimentos aplicáveis». Tribunal FISA, *Memorandum Opinion and Order* [legenda redigida] (2014), disponível em: https://www.dni.gov/files/documents/0928/FISC%20Memorandum%20Opinion%20and%20Order%2026%20August%202014.pdf.

([343]) *Ver, por exemplo,* o Relatório de conformidade do DOJ/ODNI ao FISC sobre a secção 702 da FISA para o período compreendido entre junho de 2018 e novembro de 2018, p. 21-65.

([344]) 50 U.S.C. § 1803(h). Ver também PCLOB, Sec. 702 Report, p. 76. Além disso, ver o *Memorandum Opinion and Order* do FISC de 3 de outubro de 2011 como exemplo de uma decisão relativa a deficiências em que o governo foi ordenado a corrigir as deficiências identificadas no prazo de 30 dias. Disponível em: https://www.dni.gov/files/documents/0716/October-2011-Bates-Opinion-and%20Order-20140716.pdf. Ver secção 4, «Walton Letter», p. 10-11. Ver também o parecer do FISC de 18 de outubro de 2018, disponível em: https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISC_Opin_18Oct18.pdf, confirmado pelo *Foreign Intelligence Court of Review* no seu parecer de 12 de julho de 2019, disponível em: https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_FISCR_Opinion_12Jul19.pdf, em que o FISC, entre outros aspetos, ordenou ao governo que cumprisse determinados requisitos de notificação, documentação e comunicação em relação ao FISC.

([345]) Ver, por exemplo, FISC, *Memorandum Opinion and Order at 76* (6 de dezembro de 2019) (autorizado para divulgação pública em 4 de setembro de 2020), em que o FISC instruiu o governo a apresentar um relatório escrito até 28 de fevereiro de 2020 sobre as medidas que o governo estava a tomar para melhorar os processos de identificação e eliminação de relatórios resultantes de informações recolhidas nos termos da secção 702 da FISA, que foram eliminados por motivos de incumprimento, bem como sobre outras questões. Ver também anexo VII.

da FISA. Do mesmo modo, se o FISC considerar que as certificações do governo não são suficientes, nomeadamente devido a situações de incumprimento específicas, pode emitir a chamada «decisão relativa a deficiências», exigindo que o governo corrija a violação no prazo de 30 dias ou que cesse ou não comece a aplicar a certificação prevista na secção 702. Por último, o FISC aprecia as tendências que observa nas situações de incumprimento e pode exigir alterações dos procedimentos ou supervisão e relatórios adicionais para dar resposta às tendências de cumprimento ([346]).

3.2.3. ***Reparação***

(175) Conforme explicado mais circunstanciadamente na presente secção, nos Estados Unidos existem várias vias que proporcionam aos titulares dos dados na União a possibilidade de intentar uma ação judicial num tribunal independente e imparcial com poderes vinculativos. Em conjunto, permitem que os cidadãos tenham acesso aos seus dados pessoais, que a legalidade do acesso do governo aos seus dados seja analisada e, se for detetada uma violação, que essa violação seja reparada, nomeadamente através da retificação ou apagamento dos seus dados pessoais.

(176) Em primeiro lugar, é criado um mecanismo de recurso específico nos termos do EO 14086, complementado pelo Regulamento AG que cria o *Data Protection Review Court* para tratar e resolver queixas de cidadãos relativas a atividades de informação de origem eletromagnética dos EUA. Qualquer cidadão na UE tem o direito de apresentar uma queixa ao mecanismo de recurso relativa a uma alegada violação da legislação dos EUA que rege as atividades de informação de origem eletromagnética (por exemplo, o EO 14086, a secção 702 da FISA, o EO 12333), que afete negativamente os seus interesses em matéria de privacidade e liberdades cívicas ([347]). Este mecanismo de recurso está disponível para os cidadãos de países ou de organizações regionais de integração económica designados pelo *Attorney General* dos EUA como «Estados elegíveis» ([348]). Em 30 de junho de 2023, a União Europeia e os três países da Associação Europeia de Comércio Livre que, em conjunto, constituem o Espaço Económico Europeu foram designados como «Estado elegível» ([349]) pelo *Attorney General* nos termos da secção 3, alínea f), do EO 14086. Esta designação não prejudica o disposto no artigo 42.º, n.º 2, do Tratado da União Europeia.

(177) Um titular dos dados da União que pretenda apresentar uma queixa deve apresentá-la a uma autoridade de supervisão de um Estado-Membro da UE competente para a supervisão do tratamento de dados pessoais pelas autoridades públicas (uma APD) ([350]). Tal assegura o acesso fácil ao mecanismo de recurso, permitindo que os cidadãos se dirijam a uma autoridade «próxima no seu país» e com a qual possam comunicar na sua própria língua. Após verificação dos requisitos para a apresentação de uma reclamação a que se refere o considerando 178, a APD competente encaminhará, através do secretariado do Comité Europeu para a Proteção de Dados, a reclamação para o mecanismo de recurso.

(178) A apresentação de uma queixa ao mecanismo de recurso está sujeita a requisitos de admissibilidade reduzida, uma vez que os cidadãos não precisam de demonstrar que os seus dados foram, com efeito, objeto de atividades de informação de origem eletromagnética dos EUA ([351]). Simultaneamente, para estabelecer um ponto de partida a partir do qual o mecanismo de recurso possa efetuar uma análise, devem ser fornecidas determinadas informações básicas, como, por exemplo, relativas aos dados pessoais que se acredite razoavelmente terem sido transferidos para os EUA e os meios através dos quais se acredite terem sido transferidos, as identidades das entidades do Governo dos EUA que se acredita estarem envolvidas na alegada violação (se conhecidas), o fundamento para alegar que ocorreu uma violação da legislação dos EUA (mais uma vez, tal não exige que se demonstre que os dados pessoais foram, com efeito, recolhidos pelos serviços de informações dos EUA) e a natureza da reparação requerida.

([346]) Ver anexo VII.

([347]) Ver secção 4(k)(iv) do EO 14086 que prevê que uma queixa ao mecanismo de recurso deve ser apresentada por um queixoso agindo em seu próprio nome (ou seja, não como representante de um governo, organização não governamental ou intergovernamental). A noção de «afetado» não exige que o queixoso atinja um determinado limiar para ter acesso ao mecanismo de recurso (ver considerando 178 a este respeito). Em vez disso, esclarece que o CLPO do ODNI e a DPRC têm autoridade para corrigir as violações da legislação dos EUA que rege as atividades de informação de origem eletromagnética que afetam negativamente a privacidade e os interesses em matéria de liberdades cívicas de um queixoso. Em contrapartida, as violações dos requisitos ao abrigo da legislação aplicável dos EUA que não se destinam a proteger pessoas singulares (por exemplo, requisitos orçamentais) não seriam abrangidas pela jurisdição do CLPO do ODNI e da DRPC.

([348]) Secção 3(f) EO 14086.

([349]) https://www.justice.gov/opcl/executive-order-14086.

([350]) Secção 4(d)(v) do EO 14086.

([351]) Ver secção 4(k)(i)-(iv) EO 14086.

(179) A investigação inicial das queixas apresentadas a este mecanismo de recurso é efetuada pelo CLPO do ODNI, cujas funções e poderes existentes conferidos por lei foram alargados às medidas específicas adotadas nos termos do EO 14086 ([352]). No âmbito do setor das informações, o CLPO é, entre outras funções, responsável por assegurar que a proteção das liberdades cívicas e da privacidade é adequadamente incorporada nas políticas e procedimentos do ODNI e dos serviços de informações, supervisionar o cumprimento, por parte do ODNI, dos requisitos em matéria de liberdades cívicas e privacidade aplicáveis e efetuar avaliações do impacto na privacidade ([353]). O CLPO do ODNI só pode ser destituído pelo *Director of National Intelligence* por justa causa, ou seja, em caso de má conduta, prevaricação, violação da segurança, negligência do dever ou incapacidade ([354]).

(180) Aquando da realização da sua análise, o CLPO do ODNI tem acesso à informação para a sua avaliação e pode contar com a assistência obrigatória dos responsáveis pela proteção da privacidade e das liberdades cívicas nos diferentes serviços de informações ([355]). Os serviços de informações estão proibidos de impedir ou influenciar indevidamente as análises do CLPO do ODNI, incluindo o *Director of National Intelligence*, que não deve interferir com a análise ([356]). Aquando da análise de uma queixa, o CLPO do ODNI deve aplicar a lei «imparcialmente», tendo em conta tanto os interesses de segurança nacional nas atividades de informação de origem eletromagnética como a proteção da privacidade ([357]).

(181) No âmbito da sua análise, o CLPO do ODNI determina se ocorreu uma violação da legislação dos EUA aplicável e, se for esse o caso, decide sobre uma correção adequada ([358]). Esta correção refere-se a medidas que corrigem plenamente uma violação identificada, como a cessação da obtenção ilegal de dados, a eliminação de dados recolhidos de forma ilegal, a supressão de resultados de consultas inadequadas de dados recolhidos legalmente, a restrição do acesso aos dados recolhidos legalmente ao pessoal devidamente qualificado ou a recuperação de relatórios de informações que contenham dados obtidos sem autorização legal ou que tenham sido divulgados de forma ilegal ([359]). As decisões do CLPO do ODNI sobre queixas individuais (incluindo sobre medidas corretivas) são vinculativas para os serviços de informações em causa ([360]).

(182) O CLPO do ODNI deve manter a documentação da sua análise e apresentar uma decisão classificada que explique os motivos na origem das suas conclusões factuais, da decisão sobre a ocorrência de uma violação abrangida e da determinação de eventuais medidas corretivas adequadas ([361]). Se a análise do CLPO do ODNI revelar uma violação de qualquer autoridade sujeita à supervisão do FISC, o CLPO deve também apresentar um relatório classificado ao *Assistant Attorney General for National Security*, que, por sua vez, tem a obrigação de comunicar o incumprimento ao FISC, que pode aplicar medidas coercivas adicionais (de acordo com o procedimento descrito nos considerandos 173 e 174) ([362]).

(183) Uma vez concluída a análise, o CLPO do ODNI informa o queixoso, por intermédio da autoridade nacional, de que «a análise não identificou quaisquer violações abrangidas nem o CLPO do ODNI emitiu uma decisão exigindo a aplicação de medidas corretivas adequadas ([363]).» Tal permite a proteção da confidencialidade das atividades conduzidas para proteger a segurança nacional, ao mesmo tempo que faculta às pessoas uma decisão que confirma que a sua queixa foi devidamente investigada e apreciada. Estas decisões podem ser contestadas pelas pessoas posteriormente. Para o efeito, a pessoa é informada da possibilidade de recorrer para o *Data Protection Review Court* (DPRC) para que este reaprecie as decisões do CLPO (ver considerando 184 e seguintes) e de que, no caso de o tribunal ser chamado a pronunciar-se, será selecionado um advogado especial para defender os interesses do queixoso ([364]).

([352]) Secção 3(c)(iv) do EO 14086. Ver também a *National Security Act* de 1947, 50 U.S.C. § 403-3d, secção 103D relativa ao papel do CLPO no âmbito do ODNI.
([353]) 50 U.S.C § 3029 (b).
([354]) Secção 3(c)(iv) do EO 14086.
([355]) Secção 3(c)(iii) do EO 14086.
([356]) Secção 3(c)(iv) do EO 14086.
([357]) Secção 3(c)(i)(B)(i) e (iii) do EO 14086.
([358]) Secção 3(c)(i) do EO 14086.
([359]) Secção 4(a) do EO 14086.
([360]) Secção 3(c)(d) do EO 14086.
([361]) Secção 3(c)(i)(F)-(G) do EO 14086.
([362]) Ver também secção 3(c)(i)(D) do EO 14086.
([363]) Secção 3(c)(i)(E)(1) do EO 14086.
([364]) Secções 3(c)(i)(E)(2)-(3) do EO 14086.

(184) Qualquer queixoso, bem como cada elemento do setor das informações, pode solicitar a reapreciação da decisão do CLPO do ODNI junto do *Data Protection Review Court* (DPRC). Estes pedidos de reapreciação devem ser apresentados no prazo de 60 dias após a receção da notificação da conclusão da análise pelo CLPO do ODNI e a inclusão de quaisquer informações que o cidadão pretenda fornecer ao DPRC (por exemplo, argumentos sobre questões de direito ou a aplicação da lei aos factos do processo) ([365]). Os titulares de dados da União podem voltar a apresentar o seu pedido à APD competente (ver considerando 177).

(185) O DPRC é um tribunal independente criado pelo *Attorney General* com base no EO 14086 ([366]). É constituído por, pelo menos, seis juízes nomeados pelo *Attorney General* em consulta com a PCLOB, o *Secretary of Commerce* e o *Director of National Intelligence* por mandatos renováveis de quatro anos ([367]). A nomeação dos juízes pelo *Attorney General* baseia-se nos critérios utilizados pelo poder executivo para avaliar os candidatos ao sistema judiciário federal, atribuindo um peso maior a qualquer experiência judicial anterior ([368]). Além disso, os juízes devem ser profissionais da justiça (ou seja, membros ativos e em pleno gozo dos seus direitos na Ordem dos Advogados e devidamente autorizados a exercer direito) e ter experiência adequada em matéria de direito da privacidade e da segurança nacional. O *Attorney General* deve esforçar-se por assegurar que pelo menos metade dos juízes, num dado momento, tem experiência judicial anterior e que todos os juízes possuem credenciação de segurança para poderem aceder às informações de segurança nacional classificadas ([369]).

(186) Só podem ser nomeadas para o DPRC pessoas que reúnam as condições referidas no considerando 185 e que não sejam funcionários do poder executivo no momento da sua nomeação ou que não o tenham sido nos dois anos anteriores. Do mesmo modo, durante o seu mandato no DPRC, os juízes não podem ter quaisquer funções oficiais ou emprego no Governo dos EUA (exceto como juízes no DPRC) ([370]).

(187) A independência do processo de nomeação é assegurada por diversas garantias. Em especial, o poder executivo (o *Attorney General* e os serviços de informações) está impedido de interferir ou influenciar indevidamente a apreciação do DPRC ([371]). O próprio DPRC é obrigado a apreciar os processos de modo imparcial ([372]) e funciona em conformidade com o seu próprio regulamento interno (adotado por maioria de votos). Além disso, os juízes do DPRC só podem ser destituídos pelo *Attorney General* e apenas por justa causa (ou seja, má conduta, prevaricação, violação da segurança, negligência do dever ou incapacidade), depois de ter devidamente em conta as normas aplicáveis aos juízes federais estabelecidas nas *Rules for Judicial-Conduct and Judicial-Disability Proceedings* ([373]).

([365]) Secções 201.6(a)-(b) do Regulamento AG.

([366]) Secção 3(d)(i)) e Regulamento AG. O Supremo Tribunal dos Estados Unidos reconheceu a possibilidade de o *Attorney General* criar organismos independentes com poder decisório, nomeadamente para apreciar processos individuais, ver, em especial, Estados Unidos ex rel. Accardi/Shaughnessy, 347 U.S. 260 (1954) e Estados Unidos/Nixon, 418 U.S. 683, 695 (1974). O cumprimento dos diferentes requisitos do EO 14086, por exemplo, os critérios e o procedimento de nomeação e destituição dos juízes do DRPC, está nomeadamente sujeito à supervisão do Inspetor-Geral do *Department of Justice* (ver também o considerando 109 sobre a autoridade legal dos inspetores gerais).

([367]) Secção 3(d)(i)(A) do EO 14086 e secção 201.3(a) do Regulamento AG.

([368]) Secção 201.3(b) do Regulamento AG.

([369]) Secção 3(d)(i)(B) do EO 14086.

([370]) Secção 3(d)(i)(A) do EO 14086 e secção 201.3(a) e (c) do Regulamento AG. Os candidatos nomeados para o DPRC podem participar em atividades extrajudiciais, nomeadamente atividades comerciais, financeiras, de angariação de fundos para organizações sem fins lucrativos, fiduciárias e no domínio do direito, desde que essas atividades não comprometam o exercício imparcial das suas funções ou a eficácia ou a independência do DPRC [secção 201.7(c) do Regulamento AG].

([371]) Secções 3(d)(iii)-(iv) do EO 14086 e secção 201.7(d) do Regulamento AG.

([372]) Secção 3(d)(i)(D) do EO 14086 e secção 201.9 do Regulamento AG.

([373]) Secção 3(d)(iv) do EO 14086 e secção 201.7(d) do Regulamento AG. Ver também *Bumap v United States*, 252 U.S. 512, 515 (1920), que confirmou o princípio amplamente consagrado na legislação dos EUA segundo o qual o poder de destituição decorre do poder de nomeação [tal como também recordado pelo *Office of Legal Counsel* do DoJ em *The Constitutional Separation of Powers Between the President and Congress*, 20 Op. O.L.C. 124, 166 (1996)].

(188) Os pedidos apresentados ao DPRC são apreciados por painéis de três juízes, incluindo um juiz presidente, que devem agir em conformidade com o código de conduta aplicável aos juízes dos EUA ([374]). Cada painel é assistido por um advogado especial ([375]), que tem acesso a todas as informações relativas ao processo, incluindo as informações classificadas ([376]). O papel do advogado especial é assegurar que os interesses do queixoso são representados e que o painel do DPRC está bem informado sobre todas as questões de direito e de facto pertinentes ([377]). Para melhor fundamentar a sua posição relativamente a um pedido de reapreciação apresentado junto do DPRC por um cidadão, o advogado especial pode solicitar informações ao queixoso através de perguntas escritas ([378]).

(189) O DPRC analisa as decisões tomadas pelo CLPO do ODNI (tanto se ocorreu uma violação da legislação dos EUA aplicável como no que diz respeito às medidas corretivas adequadas) com base, no mínimo, na documentação da investigação do CLPO do ODNI, bem como em quaisquer informações e pedidos apresentados pelo queixoso, pelo advogado especial ou por um serviço de informações ([379]). A formação do DPRC tem acesso a todas as informações necessárias para efetuar uma reapreciação, as quais pode obter através do CLPO do ODNI (a formação pode, por exemplo, solicitar ao CLPO para complementar a sua documentação com informações adicionais ou conclusões factuais se necessário para efetuar a reapreciação) ([380]).

(190) Aquando da conclusão da sua análise, o DPRC pode: 1) decidir que não existem provas que indiquem que ocorreram atividades de informação de origem eletromagnética envolvendo dados pessoais do queixoso, 2) decidir que as decisões do CLPO do ODNI são legalmente corretas e apoiadas por provas significativas, ou 3) se o DPRC discordar das decisões do CLPO do ODNI (se ocorreu uma violação da legislação dos EUA aplicável ou se foram aplicadas medidas corretivas adequadas), emitir as suas próprias decisões ([381]).

([374]) Secção 3(d)(i)(B) do EO 14086 e secção 201.7(a)-(c) do Regulamento AG. O *Office of Privacy and Civil Liberties* (OPCL) do *Department of Justice*, que é responsável por prestar apoio administrativo ao DPRC e aos advogados especiais (ver secção 201.5 do Regulamento AG), seleciona um painel de de três juízes numa base rotativa, procurando assegurar que cada painel inclui, pelo menos, um juiz com experiência judicial anterior (se nenhum dos juízes do painel tiver essa experiência, o juiz que preside será o juiz que o OPCL selecionou em primeiro lugar).

([375]) Secção 201.4 do Regulamento AG. O *Attorney General*, em consulta com o *Secretary of Commerce*, o *Director of National Intelligence* e a PCLOB, nomeia, pelo menos, dois advogados especiais por dois mandatos renováveis. Os advogados especiais devem ter experiência adequada no domínio do direito da privacidade e da segurança nacional, ser advogados experientes, membros ativos e em pleno gozo dos seus direitos na Ordem dos Advogados e devidamente autorizados a exercer advocacia. Além disso, no momento da sua nomeação inicial, não podem ter sido funcionários do poder executivo nos dois anos anteriores. Para cada reapreciação de um pedido, o juiz presidente seleciona um advogado especial para assistir o painel. Ver secção 201.8(a) do Regulamento AG.

([376]) Secções 201.8(c) e 201.11 do Regulamento AG.

([377]) Secção 3(d)(i)(C) do EO 14086 e secção 201.8(e) do Regulamento AG. O advogado especial não atua na qualidade de agente nem tem uma relação advogado-cliente com o queixoso.

([378]) Ver secção 201.8(d)(e) do Regulamento AG. Essas questões são, em primeiro lugar, analisadas pelo OPCL em consulta com o elemento do setor das informações competente, com vista a identificar e excluir quaisquer informações classificadas ou privilegiadas ou protegidas antes de as transmitir ao queixoso. As informações adicionais recebidas pelo advogado especial em resposta a essas questões são incluídas nos pedidos do advogado especial apresentados ao DPRC.

([379]) Secção 3(d)(i)(D) do EO 14086.

([380]) Secção 3(d)(iii) do EO 14086 e secção 201.9(b) do Regulamento AG.

([381]) Secção 3(d)(i)(E) do EO 14086 e secção 201.9(c)-(e) do Regulamento AG. De acordo com a definição de «medidas corretivas adequada» constante da secção 4, alínea a), do EO 14086, o DRPC deve ter em conta a forma como violações do mesmo tipo são habitualmente tratadas para decidir sobre uma medida corretiva aplicável ao caso em questão, ou seja, o DRPC considerará, entre outros fatores, a forma como, no passado, foram resolvidas questões de conformidade semelhantes, a fim de assegurar que a medida corretiva é eficaz e adequada.

(191) Em todos os processos, o DPRC adota uma decisão escrita por maioria de votos. Caso a reapreciação revele uma violação das regras aplicáveis, a decisão especificará as medidas corretivas adequadas, que incluem a eliminação dos dados recolhidos de forma ilegal, a supressão de resultados de consultas efetuadas de modo inadequado, a restrição do acesso aos dados recolhidos legalmente ao pessoal devidamente qualificado ou a recuperação de relatórios de informações que contenham dados obtidos sem autorização legal ou que tenham sido divulgados de forma ilegal ([382]). A decisão do DPRC é vinculativa e final no que respeita à queixa que lhe foi apresentada ([383]). Além disso, se a reapreciação revelar uma violação de qualquer autoridade sujeita à supervisão do FISC, o DPRC deve também apresentar um relatório classificado ao *Assistant Attorney General for National Security*, que, por sua vez, tem a obrigação de comunicar o incumprimento ao FISC, que pode aplicar medidas coercivas adicionais (de acordo com o procedimento descrito nos considerandos 173 e 174) ([384]).

(192) Cada decisão de um painel do DPRC é transmitida ao CLPO do ODNI ([385]). Nos processos em que a análise do DPRC for iniciada por um pedido do queixoso, este é notificado, por intermédio da autoridade nacional, de que o DPRC concluiu a sua análise e que «a análise não identificou quaisquer violações abrangidas nem o DPRC emitiu uma decisão exigindo a aplicação de medidas corretivas adequadas» ([386]). O *Office of Privacy and Civil Liberties* do DOJ mantém um registo de todas as informações apreciadas pelo DPRC e de todas as decisões proferidas, que é disponibilizado para consideração como precedente não vinculativo para futuras formações do DPRC ([387]).

(193) O DoC também é obrigado a manter um registo de cada queixoso que apresentou uma queixa ([388]). Para aumentar a transparência, o DoC deve, pelo menos de cinco em cinco anos, contactar os serviços de informações competentes para verificar se as informações relativas a uma apreciação do DPRC foram desclassificadas ([389]). Se for esse o caso, o cidadão é notificado de que essas informações podem estar disponíveis nos termos da legislação aplicável (ou seja, que este pode solicitar o acesso às mesmas ao abrigo da *Freedom of Information Act*, ver considerando 199).

(194) Por último, o funcionamento correto deste mecanismo de recurso será objeto de uma avaliação regular e independente. Mais especificamente, nos termos do EO 14086, o funcionamento do mecanismo de recurso está sujeito a uma análise anual pela PCLOB, um organismo independente (ver considerando 110) ([390]). No âmbito desta análise, a PCLOB avaliará, nomeadamente, se o CLPO do ODNI e o DPRC trataram das queixas em tempo útil, se obtiveram pleno acesso às informações necessárias, se foram tidas devidamente em conta as garantias significativas previstas no EO 14086 no processo de análise e se a comunidade de serviços de informação cumpriu, na íntegra, as decisões tomadas pelo CLPO do ODNI e pelo DPRC. A PCLOB apresentará um relatório sobre o resultado da sua análise ao Presidente, ao *Attorney General*, ao *Director of National Intelligence*, aos diretores dos serviços de informações, ao CLPO do ODNI e aos comités de informações do Congresso, que também será tornado público numa versão não classificada e que, por sua vez, contribuirá para a análise periódica do funcionamento da presente decisão que será elaborada pela Comissão. O *Attorney General*, o *Director of National Intelligence*, o CLPO do ODNI e os diretores dos serviços de informações são obrigados a aplicar ou de outro modo a abordar todas as recomendações constantes desses relatórios. Além disso, a PCLOB fará uma certificação pública anual sobre se o mecanismo de recurso está a tratar das queixas em conformidade com os requisitos constantes do EO 14086.

([382]) Secção 4(a) do EO 14086.

([383]) Secção 3(d)(ii) do EO 14086 e secção 201.9(g) do Regulamento AG. Dado que a decisão do DRPC é vinculativa e final, nenhuma outra instituição/órgão executivo ou administrativo (incluindo o Presidente dos Estados Unidos) pode anulá-la. Este princípio foi igualmente confirmado na jurisprudência do Supremo Tribunal, que esclareceu que, ao delegar a sua competência exclusiva dentro do poder executivo para tomar decisões vinculativas relativas a um órgão independente, o *Attorney General* renuncia ao poder de tomar todo o tipo de decisões em relação a esse órgão (ver *United States ex rel. Accardi v. Shaughnessy*, 347 U.S. 260 (1954).

([384]) Secção 3(d)(i)(F) do EO 14086 e secção 201.9(i) do Regulamento AG.

([385]) Secção 201.9(h) do Regulamento AG.

([386]) Secção 3(d)(i)(H) do EO 14086 e secção 201.9(h) do Regulamento AG. No que diz respeito à natureza da notificação, ver secção 201.9(a) do Regulamento AG.

([387]) Secção 201.9(j) do Regulamento AG.

([388]) Secção 3(d)(v)(A) do EO 14086.

([389]) Secção 3(d)(v) do EO 14086.

([390]) Secção 3(e) do EO 14086. Ver também https://documents.pclob.gov/prod/Documents/EventsAndPress/4db0a50d-cc62-4197-af2e--2687b14ed9b9/Trans-Atlantic%20Data%20Privacy%20Framework%20EO%20press%20release%20(FINAL).pdf.

(195) Para além do mecanismo de recurso específico criado nos termos do EO 14086, todas as pessoas têm acesso a vias de recurso (independentemente da sua nacionalidade ou local de residência) nos tribunais comuns dos EUA ([391]).

(196) Em especial, a FISA e uma lei conexa preveem a possibilidade de os cidadãos intentarem uma ação civil de indemnização contra os Estados Unidos sempre que as informações sobre si tenham sido ilegal e intencionalmente utilizadas ou divulgadas ([392]), intentarem uma ação de indemnização contra funcionários do Governo dos EUA na sua capacidade pessoal ([393]) 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 o cidadão em processos judiciais ou procedimentos administrativos tramitados nos EUA ([394]). Em termos mais gerais, se o governo tenciona utilizar informações obtidas durante operações de informações contra um suspeito num processo penal, os requisitos constitucionais e legais ([395]) impõem a obrigação de divulgar determinadas informações para que o requerido possa contestar a legalidade da recolha e utilização das provas pelo governo.

(197) Além disso, existem várias vias específicas para efeitos de recurso contra funcionários do governo em virtude do acesso ou da utilização ilegais, por parte do governo, de dados pessoais, nomeadamente para alegados efeitos de segurança nacional (ou seja, a *Computer Fraud and Abuse Act*) ([396]); a *Electronic Communications Privacy Act* ([397]); e a *Right to Financial Privacy Act* ([398])). Todas estas ações judiciais dizem respeito a dados, alvos e/ou tipos de acesso específicos (por exemplo, acesso remoto a um computador através da Internet) e estão disponíveis em determinadas condições (por exemplo, conduta intencional/deliberada, conduta fora da capacidade oficial, danos sofridos).

(198) Uma possibilidade mais geral de recurso está prevista na APA ([399]), 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 ([400]). 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» ([401]). Por exemplo, em 2015, um tribunal federal de recurso decidiu sobre um pedido submetido nos termos da APA, ou seja, que a recolha em larga escala de metadados telefónicos pelo Governo dos EUA não estava autorizada nos termos da secção 501 da FISA ([402]).

([391]) O acesso a estas vias está sujeito à demonstração da «legitimidade». Esta norma, que é aplicável a qualquer cidadão independentemente da sua nacionalidade, decorre do requisito de «caso ou controvérsia» constante do artigo III da Constituição dos EUA. De acordo com o Supremo Tribunal, este requisito exige que: 1) o cidadão tenha sofrido um «prejuízo de facto» (ou seja, um prejuízo de um interesse legalmente protegido que seja concreto e particularizado e atual ou iminente), 2) exista um nexo de causalidade entre o prejuízo e o comportamento contestado perante o tribunal, e 3) seja provável, e não especulativo, que uma decisão favorável proferida pelo tribunal resolva o prejuízo [ver Lujan/Defenders of Wildlife, 504 U.S. 555 (1992)].

([392]) 18 U.S.C. § 2712.

([393]) 50 U.S.C. § 1810.

([394]) 50 U.S.C. § 1806.

([395]) Ver *Brady/Maryland*, 373 U.S. 83 (1963) e a *Jencks Act*, 18 U.S.C. § 3500, respetivamente.

([396]) 18 U.S.C. § 1030.

([397]) 18 U.S.C. §§ 2701-2712.

([398]) 12 U.S.C. § 3417.

([399]) 5 U.S.C. § 702.

([400]) 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.

([401]) 5 U.S.C. § 706(2)(A).

([402]) *ACLU v. Clapper*, 785 F.3d 787 (2d Cir. 2015). O programa de recolha de dados telefónicos em larga escala contestado nestes processos foi encerrado com base na *FREEDOM Act* dos EUA em 2015.

(199) Por último, para além das vias de recurso referidas nos considerandos 176 a 198, qualquer cidadão tem o direito de solicitar o acesso aos registos existentes das agências federais nos termos da FOIA, nomeadamente quando estes contêm dados pessoais do cidadão ([403]). A obtenção desse acesso pode também facilitar a instauração de processos nos tribunais comuns, designadamente para demonstrar a legitimidade. Os serviços podem reter informações abrangidas por determinadas exceções específicas, nomeadamente o acesso a informações de segurança nacional classificadas e informações relativas a investigações relacionadas com a aplicação da lei ([404]), tendo, os queixosos que estejam insatisfeitos com a resposta, a possibilidade de a contestar, solicitando uma reapreciação administrativa e, posteriormente, judicial (perante os tribunais federais) ([405]).

(200) Decorre do acima exposto que quando as autoridades norte-americanas responsáveis pela aplicação da lei ou pela segurança nacional acedem aos dados pessoais abrangidos pelo âmbito de aplicação da presente decisão, tal acesso é regido por um quadro jurídico que estabelece as condições em que esse acesso pode ter lugar e assegura que o acesso e a utilização posterior dos dados se limitam ao necessário e proporcionado para o objetivo de interesse público perseguido. Estas garantias podem ser invocadas pelos cidadãos que gozem de direitos de recurso efetivos.

4. **CONCLUSÃO**

(201) A Comissão considera que os Estados Unidos — através dos princípios emitidos pelo *Department of Commerce* dos EUA — asseguram um nível de proteção dos dados pessoais transferidos da União para organizações certificadas localizadas nos Estados Unidos no âmbito do Quadro de Privacidade de Dados UE-EUA, que é essencialmente equivalente ao garantido pelo Regulamento (UE) 2016/679.

(202) Além disso, a Comissão considera que a aplicação efetiva dos princípios é assegurada por obrigações de transparência e pela administração do QPD pelo DoC. Ademais, os mecanismos de supervisão e os recursos legais previstos na legislação dos EUA permitem, no seu conjunto, identificar e punir na prática as violações às regras de proteção de dados, proporcionando vias de recurso aos titulares dos dados para terem acesso aos dados pessoais que lhes digam respeito e, eventualmente, requererem a retificação ou o apagamento desses dados.

(203) Por último, com base nas informações disponíveis sobre o quadro jurídico dos EUA, incluindo as informações constantes dos anexos VI e VII, a Comissão entende que qualquer ingerência das autoridades públicas norte-americanas no interesse público, designadamente para efeitos de aplicação do direito penal e de segurança nacional, nos direitos fundamentais dos cidadãos cujos dados pessoais sejam transferidos da União para os Estados Unidos no âmbito do Quadro de Privacidade de Dados UE-EUA, será limitada ao estritamente necessário para concretizar o objetivo legítimo em causa, existindo uma proteção jurídica eficaz contra tal ingerência. Por conseguinte, tendo em conta as conclusões referidas acima, deve ser decidido que, na aceção do artigo 45.º do Regulamento (UE) 2016/679, interpretado à luz da Carta dos Direitos Fundamentais da União Europeia, os Estados Unidos asseguram um nível de proteção adequado dos dados pessoais transferidos da União Europeia para organizações certificadas no âmbito do Quadro de Privacidade de Dados UE-EUA.

(204) Dado que as limitações, as garantias e o mecanismo de recurso criado pelo EO 14086 são elementos essenciais do quadro jurídico dos EUA no qual assenta a avaliação da Comissão, a adoção da presente decisão baseia-se, nomeadamente, na adoção de políticas e de procedimentos atualizados para aplicar o EO 14086 por todos os serviços de informações dos EUA e na designação da União como organização elegível para efeitos do mecanismo de recurso, que ocorreram, respetivamente em 3 de julho de 2023 (ver considerando 126) e 30 de junho de 2023 (ver considerando 176).

([403]) 5 U.S.C. § 552. Existem leis semelhantes a nível estadual.

([404]) Caso tal se verifique, em regra, o cidadão 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). Os critérios e a duração da classificação estão estabelecidos no EO 13526, que prevê, regra geral, que uma data ou acontecimento específico para a desclassificação deve ser estabelecido em função da duração do caráter sensível da informação para a segurança nacional, momento em que as informações devem ser automaticamente desclassificadas (ver secção 1.5 do EO 13526).

([405]) O tribunal determina de novo se os registos estão legalmente retidos e pode obrigar o governo a facultar o acesso aos registos [5 U.S. C. § 552(a)(4)(B)].

5. **EFEITOS DA PRESENTE DECISÃO E AÇÃO DAS AUTORIDADES DE PROTEÇÃO DE DADOS**

(205) Os Estados-Membros e os respetivos organismos são obrigados a tomar as medidas necessárias para cumprir os atos das instituições da União, uma vez que se presume que os mesmos são lícitos e, em consequência, produzem efeitos jurídicos até serem revogados, anulados no âmbito de um recurso de anulação ou declarados inválidos na sequência de um reenvio prejudicial ou de uma exceção de ilegalidade.

(206) Assim, uma decisão de adequação da Comissão adotada nos termos do artigo 45.º, n.o 3, do Regulamento (UE) 2016/679 é vinculativa para todos os organismos dos Estados-Membros aos quais se destina, nomeadamente para as suas autoridades de controlo independentes. Em especial, as transferências de um responsável pelo tratamento ou de um subcontratante na União para organizações certificadas localizadas nos Estados Unidos podem realizar-se sem que para tal seja necessária mais nenhuma autorização.

(207) Importa recordar que, nos termos do artigo 58.º, n.º 5, do Regulamento (UE) 2016/679, e conforme explicado pelo Tribunal de Justiça no acórdão Schrems ([406]), se uma autoridade nacional responsável pela proteção de dados colocar em causa, nomeadamente na sequência de uma queixa, a conformidade de uma decisão de adequação da Comissão com a proteção dos direitos fundamentais à privacidade e à proteção dos dados do cidadão, a legislação nacional deve proporcionar-lhe uma via de recurso que lhe permita apresentar tais objeções perante um tribunal nacional, que poderá ter de efetuar um pedido de decisão prejudicial ao Tribunal de Justiça ([407]).

6. **CONTROLO E REVISÃO DA PRESENTE DECISÃO**

(208) Em conformidade com a jurisprudência do Tribunal de Justiça ([408]), e conforme reconhecido no artigo 45.º, n.º 4, do Regulamento (UE) 2016/679, a Comissão deve controlar, de forma continuada, os desenvolvimentos pertinentes no país terceiro após a adoção de uma decisão de adequação, por forma a avaliar se o país terceiro em causa continua a assegurar um nível de proteção essencialmente equivalente. De qualquer modo, essa verificação é necessária sempre que a Comissão obtenha informações que suscitem dúvidas justificadas a esse respeito.

(209) Por conseguinte, a Comissão deve acompanhar permanentemente a situação nos Estados Unidos no que diz respeito ao quadro jurídico e à atual prática do tratamento de dados pessoais, tal como avaliado na presente decisão. Para facilitar este processo, as autoridades norte-americanas devem informar prontamente a Comissão de qualquer alteração significativa do quadro jurídico dos EUA que tenha impacto no quadro jurídico objeto da presente decisão, bem como de qualquer evolução das práticas relacionadas com o tratamento de dados pessoais avaliadas na presente decisão, tanto no que diz respeito ao tratamento de dados pessoais pelas organizações certificadas nos Estados Unidos como às limitações e às garantias aplicáveis ao acesso aos dados pessoais pelas autoridades públicas.

(210) Além disso, a fim de permitir à Comissão o exercício eficaz da sua função de controlo, os Estados-Membros devem informar a Comissão sobre qualquer medida pertinente adotada pelas autoridades nacionais responsáveis pela proteção dos dados, em particular no que se refere a consultas ou reclamações de titulares de dados da União relativas à transferência de dados pessoais da União para organizações certificadas nos Estados Unidos. A Comissão deve igualmente ser informada sobre quaisquer indícios de que as ações das autoridades públicas dos EUA responsáveis pela prevenção, investigação, deteção ou repressão de infrações penais ou pela segurança nacional, incluindo os organismos de supervisão, não asseguram o nível de proteção exigido.

([406]) Acórdão Schrems, n.º 65

([407]) Acórdão Schrems, n.º 65 Acórdão do Tribunal de Justiça, de 6 de outubro de 2015, Maximillian Schrems/Data Protection Commissioner («Schrems»), C-362/14, ECLI:EU:C:2015:650, n.º 65: «Incumbe ao legislador nacional prever vias de recurso que permitam à autoridade nacional de controlo em causa invocar as críticas que considera fundadas perante os órgãos jurisdicionais nacionais, para que estes últimos, caso partilhem das dúvidas dessa autoridade quanto à validade da decisão da Comissão, procedam a um reenvio prejudicial para efeitos da apreciação da validade dessa decisão.»

([408]) Acórdão Schrems, n.º 76

(211) Em aplicação do artigo 45.º, n.º 3, do Regulamento (UE) 2016/679 ([409]), a Comissão, após a adoção da presente decisão, deve avaliar periodicamente se as conclusões relativas à adequação do nível de proteção assegurado pelos Estados Unidos no âmbito do QPD UE-EUA continuam a ser factual e juridicamente justificadas. Uma vez que, em especial, o EO 14086 e o Regulamento AG exigem a criação de novos mecanismos e a aplicação de novas garantias, a presente decisão deve ser objeto de uma primeira avaliação no prazo de um ano após a sua entrada em vigor, para verificar se todos os elementos pertinentes foram aplicados na íntegra e se estão a funcionar eficazmente na prática. Na sequência dessa primeira avaliação e em função dos seus resultados, a Comissão decide, em estreita consulta com o comité criado nos termos do artigo 93.º, n.º 1, do Regulamento (UE) 2016/679 e o Comité Europeu para a Proteção de Dados, sobre a periodicidade das futuras revisões ([410]).

(212) Para efetuar as avaliações, a Comissão deve reunir-se com o *Department of Commerce*, com a FTC e com o DOT, acompanhados, se adequado, de outros departamentos e serviços envolvidos na aplicação do QPD UE-EUA, bem como, para as questões relativas ao acesso do governo aos dados, de representantes do DOJ, do ODNI (incluindo o CLPO), outros elementos do setor das informações, do DPRC e os advogados especiais. Essa reunião deve ser aberta à participação de representantes dos membros do Comité Europeu para a Proteção de Dados.

(213) As avaliações devem abranger todos os aspetos do funcionamento da presente decisão no que respeita ao tratamento de dados pessoais no Estados Unidos, em particular a aplicação e execução dos princípios, com especial atenção para as proteções conferidas em caso de transferências ulteriores, a evolução da jurisprudência pertinente, a eficácia do exercício dos direitos individuais, o controlo e a aplicação do cumprimento dos princípios, bem como as limitações e salvaguardas relativas ao acesso por parte do governo, nomeadamente a implementação e aplicação das salvaguardas introduzidas pelo EO 14086, incluindo através de políticas e procedimentos desenvolvidos pelos serviços de informações; a articulação entre o EO 14086 e a secção 702 da FISA e do EO 12333; e a eficácia dos mecanismos de supervisão e das vias de recurso (incluindo o funcionamento do novo mecanismo de recurso criado ao abrigo do EO 14086). No contexto dessas revisões, será também dada atenção à cooperação entre as APD e as autoridades competentes dos Estados Unidos, incluindo a elaboração de orientações e outros instrumentos interpretativos sobre a aplicação dos princípios, bem como sobre outros aspetos do funcionamento do quadro.

(214) Com base na avaliação, a Comissão deve preparar um relatório público a apresentar ao Parlamento Europeu e ao Conselho.

7. **SUSPENSÃO, REVOGAÇÃO OU ALTERAÇÃO DA PRESENTE DECISÃO**

(215) Sempre que as informações disponíveis, nomeadamente as resultantes do controlo da presente decisão ou fornecidas pelas autoridades norte-americanas ou dos Estados-Membros, revelarem que o nível de proteção conferido aos dados transferidos nos termos da presente decisão pode já não ser adequado, a Comissão deve informar sem demora as autoridades norte-americanas competentes desse facto e solicitar que sejam adotadas medidas adequadas dentro de um prazo razoável a especificar.

(216) Se, uma vez decorrido o prazo especificado, as autoridades norte-americanas competentes não tomarem essas medidas ou não demonstrarem, de forma satisfatória, que a presente decisão continua a basear-se num nível de proteção adequado, a Comissão deve dar início ao procedimento referido no artigo 93.º, n.º 2, do Regulamento (UE) 2016/679 com vista à suspensão total ou parcial ou à revogação da presente decisão.

(217) Em alternativa, a Comissão dá início a esse procedimento com vista a alterar a decisão, nomeadamente sujeitando as transferências de dados a condições adicionais ou limitando o âmbito de aplicação da verificação de adequação às transferências de dados em relação às quais continua a ser assegurado um nível adequado de proteção.

([409]) Nos termos do artigo 45.º, n.º 3, do Regulamento (UE) 2016/679, «[o] ato de execução prevê um procedimento de avaliação periódica, […] que deverá ter em conta todos os desenvolvimentos pertinentes no país terceiro ou na organização internacional».

([410]) O artigo 45.º, n.º 3, do Regulamento (UE) 2016/679 prevê a realização de uma avaliação periódica, «no mínimo de quatro em quatro anos». Ver igualmente o referencial de adequação do Comité Europeu para a Proteção de Dados, WP 254 rev. 01.

(218) Em especial, a Comissão deve iniciar o procedimento de suspensão ou revogação em caso de:

(a) Indícios de que as organizações que receberam dados pessoais da União nos termos da presente decisão não cumprem os princípios e de que esse incumprimento não é tratado de forma eficaz pelos organismos de supervisão e de aplicação da lei competentes;

(b) Indícios de que as autoridades norte-americanas não cumprem as condições e limitações aplicáveis ao acesso das autoridades públicas norte-americanas, para efeitos de aplicação da lei e de segurança nacional, aos dados pessoais transferidos no âmbito do QPD UE-EUA; ou

(c) Não resolução eficaz das queixas apresentadas pelos titulares dos dados da União, nomeadamente pelo CLPO do ODNI e/ou pelo DPRC.

(219) A Comissão deve igualmente ponderar a possibilidade de iniciar o procedimento conducente à alteração, suspensão ou revogação da presente decisão, se apurar que as autoridades norte-americanas competentes não prestam as informações ou esclarecimentos necessários à avaliação do nível de proteção conferido aos dados pessoais transferidos da União para os estados Unidos, ou no que respeita ao cumprimento da presente decisão. Nesta matéria, a Comissão deve ter em conta em que medida a informação pertinente pode ser obtida junto de outras fontes.

(220) Por imperativos de urgência devidamente justificados, por exemplo, se o EO 14086 ou o Regulamento AG forem alterados de uma forma que comprometa o nível de proteção descrito na presente decisão ou se for retirada a designação da União como organização elegível para efeitos do mecanismo de recurso por parte do *Attorney General*, a Comissão fará uso da possibilidade de adotar, de acordo com o procedimento a que se refere o artigo 93.º, n.º 3, do Regulamento (UE) 2016/679, atos de execução imediatamente aplicáveis que suspendam, revoguem ou alterem a presente decisão.

8. **CONSIDERAÇÕES FINAIS**

(221) O Comité Europeu para a Proteção de Dados publicou o seu parecer ([411]), que foi tido em conta na elaboração da presente decisão.

(222) O Parlamento Europeu adotou uma resolução sobre a adequação da proteção proporcionada pelo Quadro de Privacidade dos Dados UE-EUA ([412]).

(223) As medidas previstas ao abrigo da presente decisão estão em conformidade com o parecer do comité instituído nos termos do artigo 93.º, n.º 1, do Regulamento (UE) 2016/679.

ADOTOU A PRESENTE DECISÃO:

Artigo 1.º

Para efeitos do artigo 45.º do Regulamento (UE) 2016/679, os Estados Unidos asseguram um nível adequado de proteção dos dados pessoais transferidos da União para organizações localizadas nos Estados Unidos constantes da «lista do Quadro de Privacidade de Dados», conservada e disponibilizada publicamente pelo *Department of Commerce* dos EUA, em conformidade com o anexo I, secção I.3.

Artigo 2.º

Sempre que, para efeitos de proteção dos cidadãos no que se refere ao tratamento dos seus dados pessoais, as autoridades competentes dos Estados-Membros exercerem as suas competências, nos termos do artigo 58.º do Regulamento (UE) 2016/679 no que respeita às transferências de dados previstas no artigo 1.º da presente decisão, o Estado-Membro em causa deve informar de imediato a Comissão.

([411]) Parecer 5/2023 sobre o projeto de decisão de execução da Comissão Europeia sobre a adequação do nível de proteção dos dados pessoais assegurado pelo Quadro de Privacidade dos Dados UE-EUA de 28 de fevereiro de 2023.

([412]) Resolução do Parlamento Europeu, de 11 de maio de 2023, sobre a adequação da proteção proporcionada pelo Quadro de Privacidade dos Dados UE-EUA (2023/2501 (RSP).

Artigo 3.º

1. A Comissão assegura o controlo contínuo da aplicação do quadro jurídico objeto da presente decisão, nomeadamente as condições em que se procede a transferências ulteriores, o exercício dos direitos individuais e o acesso das autoridades públicas norte-americanas aos dados transferidos com base na presente decisão, com vista a avaliar se os Estados Unidos continuam a assegurar o nível de proteção adequado exigido por força do artigo 1.º.

2. Os Estados-Membros e a Comissão devem informar-se mutuamente dos casos em que se afigure que os organismos norte-americanos que dispõem do poder conferido pela lei para fazer cumprir os princípios estabelecidos no anexo I não fornecem mecanismos de deteção e supervisão eficazes que permitam, na prática, a identificação e sanção de infrações aos referidos princípios.

3. Os Estados-Membros e a Comissão informam-se mutuamente sobre quaisquer informações de que as interferências pelas autoridades públicas norte-americanas, responsáveis pela prossecução de objetivos de segurança nacional, pela aplicação da lei ou pela defesa de outros interesses públicos, no direito das pessoas à proteção dos seus dados pessoais vão além do estritamente necessário e proporcionado e/ou de que não existe proteção legal eficaz contra essas interferências.

4. Um ano a contar da data de notificação da presente decisão aos Estados-Membros e, posteriormente, com a periodicidade que será decidida em estreita cooperação com o Comité criado nos termos do artigo 93.º, n.º 1, do Regulamento (UE) 2016/679 e o Comité Europeu para a Proteção de Dados, a Comissão avaliará a conclusão a que se refere o artigo 1.º, n.º 1, com base em todas as informações disponíveis, incluindo as obtidas no âmbito da avaliação efetuada em conjunto com as autoridades competentes dos Estados Unidos.

5. Se a Comissão tomar conhecimento de quaisquer indícios de que deixou de ser assegurado um nível de proteção adequado, deve informar desse facto as autoridades norte-americanas competentes. Se necessário, poderá decidir suspender, alterar ou revogar a presente decisão, ou limitar o seu âmbito de aplicação, em conformidade com o disposto no artigo 45.º, n.º 5, do Regulamento (UE) 2016/679. A Comissão pode igualmente adotar a referida decisão se a falta de cooperação do governo dos EUA a impedir de apurar se os Estados Unidos continuam a assegurar um nível de proteção adequado.

Artigo 4.º

Os destinatários da presente decisão são os Estados-Membros.

Feito em Bruxelas, em 10 de julho de 2023.

Pela Comissão
Didier REYNDERS
Membro da Comissão

ANEXO I

PRINCÍPIOS DO QUADRO DE PRIVACIDADE DE DADOS UE-EUA EMITIDOS PELO DEPARTMENT OF COMMERCE DOS EUA

I. DESCRIÇÃO GERAL

1. Embora os Estados Unidos e a União Europeia (a «UE») partilhem um compromisso no sentido de reforçar a proteção da privacidade, o Estado de direito e o reconhecimento da importância dos fluxos transatlânticos de dados para os nossos cidadãos, economias e sociedades, os Estados Unidos adotam uma abordagem diferente da adotada pela UE em matéria de proteção da privacidade. Os Estados Unidos recorrem a uma abordagem setorial com base numa mescla de legislação, regulamentação e autorregulamentação. O Department of Commerce dos EUA (o *Departament*) emite os princípios do Quadro de Privacidade dos Dados UE-EUA, designadamente os princípios suplementares (coletivamente «os princípios») e o anexo I dos princípios («anexo I»), ao abrigo da sua competência jurídica para fomentar, promover e desenvolver o comércio internacional (15 USC § 1512). Os princípios foram desenvolvidos com base em consultas com a Comissão Europeia («a Comissão») e com o setor, bem como outras partes interessadas, para facilitar as relações comerciais e as transações entre os Estados Unidos e a UE. Os princípios, uma componente fundamental do Quadro de Privacidade dos Dados UE-EUA («QPD UE-EUA»), proporcionam às organizações dos Estados Unidos um mecanismo fiável para as transferências de dados pessoais da UE para os Estados Unidos, assegurando simultaneamente que os titulares de dados da UE continuam a beneficiar de garantias e proteção eficazes, tal como exigido pela legislação europeia no que diz respeito ao tratamento dos seus dados pessoais quando foram transferidos para países terceiros. Os princípios devem ser utilizados exclusivamente pelas organizações dos Estados Unidos que recebem dados pessoais da UE para serem elegíveis para o QPD UE-EUA e, portanto, beneficiarem da decisão de adequação da Comissão Europeia ([1]). Os princípios não afetam a aplicação do Regulamento (UE) 2016/679 (Regulamento Geral sobre a Proteção de Dados ou RGPD) ([2]) que é aplicável ao tratamento de dados pessoais nos Estados-Membros da UE. 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 QPD UE-EUA para efetuar transferências de dados pessoais da UE, as organizações devem autocertificar a sua adesão aos princípios ao *Department* (ou ao seu representante). Portanto, embora a decisão das organizações de aderirem ao QPD UE-EUA seja estritamente voluntária, a conformidade efetiva é obrigatória: as organizações que autocertificam ao *Department* e declaram publicamente o seu compromisso de aderir aos princípios devem cumpri-los na íntegra. Para aderir ao QPD UE-EUA, uma organização deve a) estar sujeita aos poderes de investigação e execução da *Federal Trade Commission* («FTC»), do *Department of Transportation* dos EUA («DOT») 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 conformes com estes princípios; e d) aplicá-los na íntegra ([3]). O incumprimento por parte de uma organização pode ser sujeito a medidas coercivas pela FTC nos termos da Secção 5 da *Federal Trade Commission Act* (FTC), que proíbe atos desleais e desonestos praticados no comércio ou que o afetem (15 U.S.C. § 45); pelo DOT, nos termos do título 49 U.S.C. § 41712, que proíbe uma transportadora ou agente de viagens de adotar práticas desleais ou enganosas no transporte aéreo ou na venda de passagens aéreas; ou ao abrigo de outras leis ou regulamentos que proíbam tais atos.

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

([2]) 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).

([3]) Os princípios do quadro do Escudo de Proteção da Privacidade UE-EUA foram alterados e são designados «princípios do Quadro de Privacidade dos Dados UE-EUA». (*Ver* princípio suplementar em matéria de autocertificação).

3. O *Department* manterá e disponibilizará ao público uma lista oficial das organizações dos EUA que autocertificaram a sua adesão ao *Department*, bem como o seu compromisso de aderir aos princípios («a lista Quadro de Privacidade dos Dados»). Os benefícios do QPD UE-EUA são assegurados a partir da data em que o *Department* inscreve a organização na lista do Quadro de Privacidade dos Dados. O *Department* retirará da Lista do Quadro de Privacidade dos Dados as organizações que se retirem voluntariamente do QPD UE-EUA ou não concluam a sua recertificação anual ao *Department*; estas organizações devem continuar a aplicar os princípios às informações pessoais que receberam ao abrigo do QPD UE-EUA e confirmar anualmente ao *Department* o seu compromisso de o fazer (ou seja, enquanto conservarem essas informações), assegurar uma proteção «adequada» das informações por outro meio autorizado (por exemplo, utilizando um contrato que reflita plenamente os requisitos das cláusulas contratuais-tipo pertinentes adotadas pela Comissão) ou devolver ou apagar as informações. O *Department* também suprimirá da lista do Quadro de Privacidade dos Dados as organizações que sistematicamente não tenham cumprido os princípios; estas organizações devem devolver ou apagar as informações pessoais que receberam ao abrigo do QPD UE-EUA. A supressão de uma organização da lista do Quadro de Privacidade dos Dados significa que esta deixa de poder beneficiar da decisão de adequação da Comissão para receber informações pessoais da UE.

4. O *Department* também manterá e disponibilizará ao público um registo oficial das organizações dos EUA que autocertificaram previamente a sua adesão ao *Department*, mas que foram suprimidas da lista do Quadro de Privacidade dos Dados. O *Department* emitirá um aviso claro no sentido de que estas organizações não participam no QPD UE-EUA; que a supressão da lista do Quadro de Privacidade dos Dados significa que estas organizações não podem alegar respeitar o Quadro de Privacidade dos Dados e devem evitar todas as declarações ou práticas enganosas que sugiram que participam no QPD UE-EUA; e que tais organizações já não têm o direito a beneficiar da decisão de adequação da Comissão que lhes permitiria receber informações pessoais da UE. Uma organização que continue a alegar participar no QPD UE-EUA ou que apresente outras declarações falsas relacionadas com o QPD UE-EUA depois de ter sido suprimida da lista do Quadro de Privacidade dos Dados pode ser objeto de medidas coercivas por parte da FTC, do DOT ou de outros organismos de execução.

5. A adesão a estes princípios pode ser limitada: a) na medida do necessário para dar cumprimento a uma decisão judicial ou observar requisitos de segurança nacional, interesse público e aplicação da lei, nomeadamente nos casos em que legislação ou regulamentação governamental criem obrigações contraditórias; b) por legislação, decisão judicial ou regulamento governamental que gerem autorizações explícitas, desde que, no exercício dessa 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) se o efeito do RGPD for permitir exceções ou derrogações, nas condições nele estabelecidas, desde que essas exceções ou derrogações sejam aplicadas em contextos comparáveis. Neste contexto, as salvaguardas previstas na legislação dos EUA para proteger a privacidade e as liberdades cívicas incluem as exigidas pelo EO 14086 ([4]) nas condições nele estabelecidas (incluindo os seus requisitos em matéria de necessidade e proporcionalidade). 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, comprometendo-se, nomeadamente, a indicar, nas respetivas políticas de proteção da vida privada, os casos em que se apliquem exceções aos princípios permitidas pela alínea b) supra. 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 QPD UE-EUA após a adesão ao mesmo. Uma organização que opte por aplicar os princípios do QPD UE-EUA 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*, em conformidade com o disposto no princípio suplementar sobre autocertificação.

([4]) Decreto Presidencial de 7 de outubro de 2022, «Enhancing Safeguards for United States Signals Intelligence Activities.»

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 QPD UE-EUA, à exceção de casos em que essas 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 do RGPD 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, qualquer operação ou conjunto de operações sobre dados pessoais, efetuadas com ou sem meios automatizados, 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 e do anexo I dos princípios é a data de entrada em vigor da decisão de adequação da Comissão Europeia.

II. **PRINCÍPIOS**

1. **AVISO**

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

   i. a sua participação no QPD UE-EUA e fornecer uma ligação para a lista do Quadro de Privacidade dos Dados,

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

   iii. o seu compromisso de submeter aos princípios todos os dados pessoais recebidos da UE com base no QPD UE-EUA,

   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 DOT ou de qualquer outro organismo público autorizado dos EUA,

   xi. a possibilidade de, em determinadas condições, o cidadão solicitar arbitragem vinculativa ([5]),

   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.

([5]) *Ver, por exemplo,* a secção (c) do princípio de recurso, aplicação e responsabilidade.

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 (isto é, *opt out* — opção de não participação) se os seus dados pessoais podem: 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 (isto é, *opt in*) dos cidadãos, caso se pretenda i) divulgar a informação a terceiros ou ii) utilizá-la para uma finalidade 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*, 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 ([6]). Uma organização não pode tratar informações pessoais de um modo incompatível com os objetivos que motivaram a recolha ou com os objetivos autorizados posteriormente pela 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 conservadas sob uma forma identificável ou de identificação ([7]) individual enquanto serve uma finalidade de tratamento na aceção do n.º 5-A. Esta obrigação não obsta a que as organizações tratem 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 aos outros princípios e disposições do QPD UE-EUA. 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.

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* sobre o QPD UE-EUA. 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*. 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.

([6]) 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.

([7]) 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.

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 são responsáveis pelo tratamento das informações pessoais que recebem ao abrigo do QPD UE-EUA e transferem posteriormente para um terceiro que desempenha a função de agente em seu nome. A organização aderente 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. Quando uma organização ficar sujeita a uma decisão judicial motivada por incumprimento ou a uma decisão de um organismo oficial dos EUA (por exemplo, FTC ou DOT) enumerado nos princípios ou num futuro anexo aos princípios igualmente motivada por incumprimento, a organização deve tornar públicas todas as secções pertinentes relacionadas com o QPD UE-EUA de qualquer relatório de conformidade ou avaliação apresentado ao tribunal ou organismo oficial dos EUA, na medida em que tal seja compatível com os requisitos de confidencialidade. O *Department* criou um ponto de contacto específico ao qual as APD podem recorrer em caso de problemas de conformidade por parte das organizações aderentes. A FTC e o DOT darão prioridade às queixas de incumprimento dos princípios recebidas do *Department* e das autoridades dos Estados-Membros da UE e procederão 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 (isto é, 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, 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.

3. Responsabilidade subsidiária

a. Os fornecedores de serviços da Internet (ISP), os operadores de telecomunicações e outras organizações não estão sujeitos aos princípios quando, em nome de outra organização, se limitam a transmitir, encaminhar, trocar ou guardar informação. O QPD UE-EUA 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, são regularmente objeto de auditorias. Estas auditorias, designadamente as que investigam potenciais irregularidades, podem ser prejudicadas se forem divulgadas prematuramente. Igualmente, uma organização aderente 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 cumprirão o seu compromisso de cooperação com as APD do modo descrito abaixo. Em conformidade com o QPD UE-EUA, as organizações norte-americanas que recebam dados pessoais provenientes da UE devem comprometer-se a utilizar mecanismos eficazes que garantam o cumprimento dos princípios. Mais especificamente, tal como estabelecido no princípio de recurso, aplicação e responsabilidade, as organizações participantes devem proporcionar o seguinte: a) i) recurso para as pessoas a quem os dados dizem respeito, a) ii) procedimentos de acompanhamento para verificar a veracidade das declarações e afirmações que fizeram sobre as respetivas práticas em matéria de privacidade, e a) iii) a obrigação de solucionar problemas decorrentes do incumprimento dos princípios por essas organizações e consequências para essas organizações. 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 QPD UE-EUA dirigida ao *Department* (ver princípio suplementar sobre autocertificação) que:

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

ii. cooperará com as APD na investigação e na resolução de queixas formuladas no âmbito dos princípios; e

iii. respeitará as decisões das APD, sempre que estas considerem que a organização deve tomar medidas específicas para cumprir os princípios, 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 informal de APD composto por estas autoridades à escala da UE, 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 por pessoas cuja informação pessoal, transferida da UE ao abrigo do QPD UE-EUA, tenha sido objeto de tratamento. Esse aconselhamento, que tem por fim garantir a correta aplicação dos princípios, 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 QPD UE-EUA, 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 remeter o caso para a FTC, o DOT ou outro organismo federal ou estadual norte-americano com competência para tomar medidas coercivas em caso de fraude ou prestação de falsas declarações, ou para concluir que o Acordo de Cooperação foi seriamente violado devendo, por isso, ser considerado nulo. Nesta última hipótese, o painel informará o *Department* para que seja alterada a lista do Quadro de Privacidade dos Dados. Qualquer violação do acordo de cooperação com as APD, bem como dos princípios, será objeto de recurso ao abrigo da secção 5 da FTC Act (15 U.S.C. § 45, 49 U.S.C. § 41712,) (ou de outra lei semelhante.

d. Se a organização desejar que a sua adesão ao QPD UE-EUA abranja também os dados relativos a recursos humanos transferidos da UE para serem utilizados num contexto de relações de trabalho 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 optem por esta opção terão de pagar uma taxa anual, que será destinada a cobrir os custos de funcionamento do painel. Podem, além disso, ser chamadas a suportar as despesas de tradução necessárias decorrentes da apreciação, pelo painel, das consultas ou queixas contra eles apresentadas. O montante da taxa será determinado pelo *Departament* após consulta da Comissão. A cobrança da taxa pode ser efetuada por um terceiro selecionado pelo *Departament* para exercer a função de depositário dos fundos cobrados para este efeito. O *Departament* cooperará estreitamente com a Comissão e as APD no estabelecimento de procedimentos adequados para a distribuição dos fundos cobrados através da taxa, bem como de outros aspetos processuais e administrativos do painel. O *Departament* e a Comissão podem acordar em alterar a frequência com que a taxa é cobrada.

6. **Autocertificação**

a. Os benefícios do QPD UE-EUA são assegurados a partir da data em que o *Department* inscreve a organização na lista do Quadro de Privacidade dos Dados. O *Department* só colocará uma organização na lista do Quadro de Privacidade dos Dados depois de ter determinado que a apresentação inicial de autocertificação da organização está completa, e eliminará a organização dessa lista se esta se retirar voluntariamente, não concluir a sua recertificação anual ou não cumprir sistematicamente os princípios (ver o princípio suplementar em matéria de resolução e execução de litígios).

b. Para se autocertificar inicialmente ou se recertificar posteriormente para o QPD UE-EUA, uma organização deve, em cada caso, fornecer ao *Department* uma declaração de um responsável da empresa em nome da organização que procede à autocertificação ou recertificação (conforme aplicável) da sua adesão aos princípios ([8]), que contenha, pelo menos, as seguintes informações:

([8]) A declaração deve ser apresentada através do sítio Web do Quadro de Privacidade dos Dados do *Department* por uma pessoa da organização autorizada a fazer declarações em nome da organização e de qualquer uma das suas entidades abrangidas relativamente à sua adesão aos princípios.

i. o nome da organização norte-americana que se autocertifica ou recertifica, bem como o(s) nome(s) de qualquer uma das suas entidades ou filiais norte-americanas que também adira aos princípios que a organização pretende abranger;

ii. uma descrição das atividades da organização em matéria de dados pessoais que seriam recebidos da UE ao abrigo do QPD UE-EUA;

iii. uma descrição da política pertinente da organização em matéria de proteção da vida privada no que diz respeito a esses dados pessoais, 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; e

2. a sua data de aplicação;

iv. o nome do gabinete de contacto dentro da organização responsável pelo tratamento de queixas, pedidos de acesso ou quaisquer outros assuntos relacionados com os princípios ([9]), designadamente:

1. o(s) nome(s), cargo(s) (conforme aplicável), endereço(s) eletrónico(s) e número(s) de telefone da(s) pessoa(s) pertinente(s) ou do(s) serviço(s) de contacto relevante(s) dentro da organização; e

2. o endereço postal pertinente da organização nos EUA;

v. 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);

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

vii. o método de verificação (ou seja, autoavaliação; ou fora do âmbito das verificações de conformidade, incluindo o terceiro que as realiza) ([10]); e

viii. o(s) mecanismo(s) de recurso independente(s) pertinente(s) disponível (eis) para investigar queixas por resolver relacionadas com os princípios ([11]).

c. Se a organização desejar que a sua adesão ao DPD UE-EUA abranja também a informação relativa a recursos humanos transferida da UE para ser utilizada num contexto de relações de trabalho 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 inicial, bem como em eventuais declarações de recertificação, 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* 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.

([9]) O principal «contacto da organização» ou o «responsável institucional da organização» não podem ser externos à organização (por exemplo, um conselheiro ou consultor externo).

([10]) Ver princípio suplementar sobre verificação.

([11]) *Ver* princípio suplementar sobre resolução de litígios e aplicação.

d. O Department manterá e publicará a lista do Quadro de Privacidade dos Dados das organizações que apresentaram pedidos de autocertificação completos e atualizará essa lista com base nas declarações de recertificação anuais completas, bem como nas notificações recebidas em conformidade com o princípio suplementar em matéria de resolução de litígios e aplicação. Estas declarações de recertificação deverão ser apresentadas, no mínimo, uma vez por ano; caso contrário, as organizações serão suprimidas da lista do Quadro de Privacidade dos Dados e deixarão de usufruir dos benefícios decorrentes do QPD UE-EUA. Todas as organizações que o *Department* incluir na lista do Quadro de Privacidade dos Dados devem ter políticas de proteção da privacidade pertinentes que respeitem o princípio de aviso e indicar, nessas políticas de privacidade, que respeitam os princípios ([12]). 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* relativo ao Quadro de Privacidade dos Dados 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 relacionadas com os princípios sem custos para a pessoa em causa.

e. Os princípios devem ser aplicáveis imediatamente após a autocertificação. As organizações participantes que anteriormente se autocertificaram em conformidade com os princípios do quadro do Escudo de Proteção da Privacidade UE-EUA terão de atualizar as respetivas políticas em matéria de privacidade de forma a referirem os «Princípios do Quadro de Privacidade dos Dados UE-EUA». Essas organizações devem incluir esta referência o mais rapidamente possível e, em qualquer caso, o mais tardar três meses a contar da data em que os princípios do Quadro de Privacidade dos Dados UE-EUA produzem efeitos.

f. Uma organização deve submeter aos princípios todos os dados pessoais recebidos da UE com base no QPD UE-EUA. O compromisso de adesão aos princípios não se limita apenas aos dados pessoais recebidos durante o período em que a organização usufrui dos benefícios decorrentes do QPD UE-EUA; 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 retirar-se do QPD UE-EUA. Uma organização que pretenda retirar-se do QPD UE-EUA deve notificar previamente o *Departament* desse facto. Esta notificação deve também indicar o que a organização pretende fazer com os dados pessoais que recebeu com base no QPD UE-EUA (ou seja, conservar, devolver ou apagar os dados e, se os conservar, os meios autorizados que utilizará para assegurar a sua proteção). Uma organização que se retire do QPD UE-EUA, mas que deseje conservar os referidos dados, deve confirmar anualmente ao *Department* o seu compromisso de continuar a aplicar os princípios ou proporcionar uma proteção «adequada» dos dados 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); caso contrário, a organização deve devolver ou apagar as informações ([13]). Uma organização que ser retire do QPD UE-EUA 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 nele participar ativamente e tem direito aos benefícios que proporciona.

([12]) Uma organização que se autocertifique pela primeira vez não pode alegar a participação no QPD UE-EUA na sua política de privacidade final até que o *Department* a notifique de que o pode fazer. Aquando da apresentação da sua declaração de autocertificação inicial, a organização deve fornecer ao *Department* um projeto de política de privacidade que seja coerente com os princípios. Uma vez que o *Department* tenha determinado que a apresentação inicial da autocertificação da organização está completa, notificará a organização de que deve finalizar (por exemplo, publicar, se for caso disso) a sua política de proteção da privacidade coerente com o QPD UE-EUA. A organização deve notificar o *Department* logo que a política de privacidade pertinente esteja concluída, data em que o *Department* incluirá a organização na lista do Quadro de Privacidade dos Dados.

([13]) Se, no momento da sua retirada, uma organização optar por conservar os dados pessoais que recebeu com base no QPD UE-EUA e confirmar anualmente ao *Department* que continua a aplicar os princípios a esses dados, a organização deve comunicar ao *Department* uma vez por ano após a sua retirada (ou seja, a menos e até que a organização proporcione uma proteção «adequada» desses dados por outro meio autorizado, ou devolva ou apague todos esses dados e notifique o *Department* dessa ação) o que fez com esses dados pessoais, o que fará com qualquer desses dados pessoais que continue a conservar e quem servirá de ponto de contacto permanente para questões relacionadas com os princípios.

g. Uma organização que cesse de existir como entidade jurídica separada devido a uma alteração do seu estatuto jurídico, na sequência de uma fusão, aquisição, falência ou dissolução, deve antecipadamente informar desse facto o *Department*. A notificação deve igualmente indicar se a entidade resultante da alteração do estatuto jurídico i) continuará a participar no QPD UE-EUA através de uma autocertificação existente; ii) se autocertificará como nova organização participante no QPD UE-EUA (por exemplo, se a nova entidade ou entidade sobrevivente não dispuser já de uma autocertificação através da qual possa participar no QPD UE-EUA); ou iii) estabelecer outras garantias, tais como um acordo escrito que garanta a continuação da aplicação dos princípios a quaisquer dados pessoais que a organização tenha recebido ao abrigo do QPD UE-EUA e que sejam conservados. Quando nenhuma destas condições, i), ii) ou iii), se aplicar, quaisquer dados pessoais que tenham sido recebidos no âmbito do QPD UE-EUA devem ser prontamente devolvidos ou apagados.

h. Sempre que uma organização se retire do QPD UE-EUA por algum motivo, deve apagar todas as declarações que sugiram que a organização continua a participar no referido quadro ou que tem direito aos benefícios que este proporciona. A marca de certificação do QPD UE-EUA, se utilizada, também deve ser removida. Qualquer declaração falsa prestada ao público relativa à adesão de uma organização aos princípios poderá ser objeto de recurso junto da FTC, do DOT ou de qualquer outra instância governamental competente. As declarações falsas prestadas ao *Department* poderão ser objeto de recurso ao abrigo da False Statements Act (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 QPD UE-EUA, correspondem à verdade, como também se essas práticas em matéria de privacidade foram aplicadas em conformidade com as declarações prestadas e com os princípios.

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. Nos casos em que a organização optou pela autoavaliação, essa verificação deve demonstrar que a sua política em matéria de privacidade relativamente às informações pessoais recebidas da UE é exata, exaustiva, facilmente disponível, conforme com os princípios e plenamente aplicada (ou seja, está a ser cumprida). Deve igualmente indicar que os cidadãos estão informadas sobre os instrumentos internos específicos de que a organização dispõe para o tratamento de queixas e sobre o(s) mecanismo(s) de recurso independentes de apresentação de queixas; que a organização instituiu procedimentos para 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 de que a autoavaliação, foi preenchida deve ser assinada por um responsável da empresa, ou por qualquer outro representante autorizado da organização, no mínimo, uma vez por ano e posta à disposição dos cidadãos, mediante pedido ou no âmbito de uma investigação ou de queixa por motivos de não conformidade.

d. Se a organização optar por uma verificação de conformidade externa, essa verificação deve demonstrar que a sua política de privacidade relativa às informações pessoais recebidas da UE é exata, abrangente, de fácil acesso, está em conformidade com os princípios e plenamente implementada (*ou seja*, está a ser cumprida). Deve indicar ainda que os cidadãos são informados do(s) mecanismo(s) através do(s) qual(ais) podem apresentar queixas. 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 que comprova 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 dos cidadãos, 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 QPD UE-EUA, que devem ser postos à disposição, mediante pedido, no âmbito de uma investigação ou queixa relativa à conformidade, do organismo independente de resolução de litígios 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* sobre a adesão da organização aos princípios.

8. **Acesso**

a. O princípio de acesso na prática

i. No âmbito dos princípios, o direito de acesso é fundamental para a proteção da privacidade. Permite, em especial, que os cidadãos verifiquem a exatidão das informações que outras entidades possuem a seu respeito. O princípio de acesso significa que os cidadãos têm direito a:

1. obter de uma organização a confirmação de se a organização procede ao tratamento dos seus dados pessoais ([14]);

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 violação aos princípios.

ii. Os cidadãos não são obrigados a justificar um pedido de acesso aos seus dados pessoais. Ao satisfazer os pedidos de acesso por parte dos cidadãos, as organizações devem orientar-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 o cidadão 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 ao cidadão 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 em situações que impliquem a violação dos direitos legítimos de terceiros ou os encargos ou as despesas para facultar esse acesso forem desproporcionados em relação aos riscos para a privacidade do cidadão 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.

ii. Se a informação pessoal for utilizada para tomar decisões que poderão afetar significativamente o cidadão 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 o cidadão, 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.

([14]) 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. 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 pertinentes 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 esse acesso são limitadas e quaisquer razões apresentadas para justificar a recusa devem ser específicas. Conforme estabelecido pela 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 aos cidadãos 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 o cidadão em causa se propuser pagá-los.

g. Pedidos de acesso repetidos ou abusivos

i. Uma organização pode estabelecer limites razoáveis de resposta para o número de vezes que um dado cidadão apresenta pedidos de acesso num determinado período. Aquando da fixação destes limites, uma organização deve considerar fatores como a frequência com que a informação é atualizada, a finalidade para a qual os dados são utilizados e a natureza da informação.

h. Pedidos de acesso fraudulentos

i. 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

i. 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 QPD UE-EUA

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 QPD UE-EUA, a transferência goza das condições garantidas por este quadro. Nestes casos, a recolha de informação e o seu tratamento antes de efetuada a transferência devem ter sido sujeitos à legislação nacional do Estado-Membro da UE onde se processou a recolha, bem como às condições ou restrições impostas à transferência que devem ser respeitadas de acordo com essa mesma legislação.

ii. Os princípios 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 anonimizados não levanta quaisquer preocupações em matéria de privacidade.

b. Aplicação dos princípios de aviso e escolha

i. Uma organização norte-americana que receba informações abrangidas pelo QPD UE-EUA, 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, como, para fins de comunicações de *marketing*, a organização norte-americana deve, antes de mais, garantir aos cidadãos em causa o direito de escolha necessário, a não ser que estas tenham já autorizado o uso da informação para esses fins. Essa utilização não deve ser incompatível com os fins para os quais os dados pessoais foram recolhidos ou ulteriormente autorizados pelo cidadão 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, anonimizar 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 necessários para não prejudicar a capacidade da organização em matéria de promoções, nomeações ou outras decisões de índole semelhante.

c. Aplicação do princípio de acesso

i. 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 QPD UE-EUA requer 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 continua a ser 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. 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 QPD UE-EUA que utilize os dados relativos aos recursos humanos da UE transferidos da UE, no âmbito das relações de trabalho, e que pretenda que essas transferências sejam abrangidas pelo QPD UE-EUA tem, por conseguinte, de se comprometer a colaborar em qualquer investigação e a agir em conformidade com as orientações das autoridades da UE competentes nesses casos.

e. Aplicação do princípio de responsabilização pela transferência ulterior

i. No que diz respeito a necessidades operacionais ocasionais relacionadas com o emprego das organizações aderentes ao QPD UE-EUA no que se refere aos dados pessoais transferidos no âmbito deste quadro, 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 responsabilização 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 QPD UE-EUA.

ii. Na UE, os responsáveis pelo tratamento de dados são sempre obrigados a celebrar um contrato quando se efetua uma transferência para tratamento (subcontratação), quer esta ocorra no interior ou no exterior da UE e independentemente de o responsável pelo tratamento participar no QPD UE-EUA. 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 alteração, 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. Dado que as organizações participantes asseguram uma proteção adequada, os contratos com essas organizações para simples tratamento não exigem autorização prévia.

b. Transferências num grupo controlado de empresas ou entidades

i. Nos casos em forem 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 responsabilização pela transferência ulterior. Os responsáveis pelo tratamento dos dados num grupo controlado de empresas ou entidades podem basear estas transferências noutros instrumentos, 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 permanece responsável pelo cumprimento dos princípios.

c. Transferências entre responsáveis pelo tratamento de dados

i. 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 aderente nem que disponha de um mecanismo de recurso independente. A organização aderente deve celebrar um contrato com o terceiro responsável pelo tratamento de dados que preveja o mesmo nível de proteção que o garantido pelo QPD UE-EUA, não incluindo o requisito de que o terceiro responsável pelo tratamento de dados deve ser uma organização aderente ao QPD UE-EUA 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 QPD UE-EUA. O princípio suplementar sobre verificação estabelece como cumprir os requisitos da alínea a), subalínea ii), do princípio. Este princípio suplementar considera as disposições da alínea a), subalíneas i) e iii), que requerem 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 nas suas regras e que incluam mecanismos de aplicação 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 a resolução de litígios; ou iii) comprometendo-se a cooperar com as APD da UE ou com 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. Note-se 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 *FTC Act* que proíbe atos desleais ou enganosos (15 U.S. C. § 45), 49 U.S.C. § 41712, que proíbe uma transportadora ou uma agência de viagens de praticar práticas desleais ou enganosas no transporte aéreo ou na venda de passagens aéreas, ou outras disposições legislativas ou regulamentares que proíbam tais atos.

c. A fim de contribuir para assegurar o cumprimento dos seus compromissos relativos ao QPD UE-EUA e apoiar a administração do programa, as organizações, bem como os respetivos mecanismos de recurso independentes, devem prestar informações sobre o QPD UE-EUA sempre que estas sejam solicitadas pelo *Department*. Além disso, as organizações devem responder com celeridade às queixas relativas à sua conformidade com os princípios transmitidas através do *Department* pelas APD. A resposta deve indicar se a queixa é fundamentada e, em caso afirmativo, as medidas que a organização aplicará para sanar 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, os cidadãos devem ser encorajados a apresentar quaisquer queixas que possam ter à organização em causa, antes de recorrerem a mecanismos de recurso independentes. As organizações devem responder aos cidadãos 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, pela sua imparcialidade, pela sua transparência da composição e pelo seu financiamento, bem como pela sua experiência comprovada. Como exigido pelo princípio de recurso, aplicação e responsabilidade, o recurso colocado à disposição dos cidadãos deve ser de fácil utilização e gratuito. Os organismos independentes para a resolução de litígios devem investigar cada uma das queixas apresentadas pelos cidadãos, a menos que se trate de queixas infundadas ou abusivas, o que não impedirá que o organismo independente de resolução de litígios 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. Além disso, os mecanismos de recurso devem facultar aos cidadãos, 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. 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 QPD UE-EUA, bem como os serviços que prestam no seu âmbito. Estas informações devem incluir: 1) informações sobre os requisitos dos princípios em matéria de mecanismos de recurso independentes ou uma hiperligação para os mesmos; 2) uma hiperligação para o sítio Web relativo ao Quadro de Privacidade de Dados do *Department*; 3) um esclarecimento de que os seus serviços de resolução de litígios no âmbito do QPD UE-EUA são gratuitos para os cidadãos; 4) uma descrição de como é possível apresentar uma queixa relacionada com os princípios; 5) o prazo para o tratamento das queixas relacionadas com os princípios; 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 os princípios 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. Conforme 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 violou as suas obrigações para com o cidadão nos termos dos princípios, e se essa 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 ([15]) ou no respeitante a uma alegação sobre a adequação do QPD UE-EUA. No âmbito desta opção de arbitragem, o «Comité do quadro de privacidade de dados UE-EUA» (constituído por um ou três árbitros, conforme o acordado pelas partes) tem competência para aplicar medidas equitativas, não pecuniárias e específicas do cidadão (como acesso, correção, eliminação ou devolução dos dados do cidadão em questão) necessárias para reparar a violação dos princípios apenas no que se refere ao cidadão. Os cidadãos e as organizações aderentes 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).

e. Reparação e sanções

i. O resultado de quaisquer reparações decididas pelo organismo independente de 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 oportuno, deixar de proceder ao tratamento dos dados pessoais do cidadão que apresentou queixa. As sanções devem ser suficientemente rigorosas de modo a assegurar que a organização cumpre os 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

([15]) *The Principles, Overview,* n.º 5.

determinadas circunstâncias ([16]). Outras sanções podem consistir na suspensão ou retirada de autorização, em compensações a cidadãos que sofram perdas decorrentes de não conformidade e injunções. Os organismos de autorregulamentação e os organismos independentes de resolução de litígios do setor privado devem informar os tribunais ou as entidades governamentais com competência na matéria, sempre que tenham conhecimento de violação das regras por parte das organizações aderentes, bem como o *Department*.

f. Atividade da FTC

i. A FTC comprometeu-se a examinar prioritariamente as queixas em matéria de incumprimento apresentadas: i) por organismos de autorregulamentação em matéria de privacidade e por outros organismos independentes para a resolução de litígios; ii) por Estados-Membros da UE; e iii) pelo *Department*, para determinar se há violação da secção 5 da *FTC 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 QPD UE-EUA ou de participação no referido quadro por organizações que já não constam da lista do QPD UE-EUA ou que nunca autocertificaram a sua adesão ao *Department*. 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* 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.

g. Incumprimento persistente

i. Caso determinada organização persista em não cumprir os princípios, deixará de beneficiar do QPD UE-EUA. As organizações que, de maneira persistente, não tenham cumprido os princípios devem ser suprimidas da lista do QPD UE-EUA pelo *Department* e devem devolver ou eliminar as informações pessoais recebidas no âmbito do referido quadro.

ii. O incumprimento recorrente ocorre sempre que uma organização que tenha apresentado ao *Department* a respetiva autocertificação recuse cumprir a decisão final de um organismo privado de autorregulamentação, de um organismo independente de resolução de litígios ou de uma entidade pública, ou que um desses organismos, nomeadamente o *Department*, constate que uma organização desrespeita frequentemente os princípios, a ponto de o seu empenho no cumprimento dos princípios deixar de ser credível. Nos casos em que essa determinação é efetuada por um organismo que não o *Department*, a organização deve notificar imediatamente esse facto ao *Department*. Se não o fizer sujeitar-se-á a processo judicial nos termos da False Statements Act (18 U.S.C. § 1001). O abandono por parte de uma organização de um programa de autorregulamentação em matéria de 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* suprimirá uma organização da lista do Quadro de Privacidade de Dados por incumprimento persistente, nomeadamente em resposta a qualquer notificação que receba desse incumprimento da própria organização, de um organismo de autorregulamentação em matéria de privacidade ou de outro organismo independente de resolução de litígios ou de um organismo público, mas só após notificar a organização com 30 dias de antecedência e de lhe dar a oportunidade de responder ([17]). De igual modo, a lista do Quadro de Privacidade de Dados do *Department* 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 QPD UE-EUA, deverá facultar a esse organismo todas as informações referentes à sua participação anterior no referido quadro.

([16]) Os organismos independentes de 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.

([17]) O *Department* indicará no aviso o prazo, que será necessariamente inferior a 30 dias, para a organização responder ao aviso.

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 do cidadão em causa. Por conseguinte, um cidadão 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 do cidadão que solicita a não participação. Nos Estados Unidos, os cidadãos podem exercer esta opção através de um programa central de «não participação». Em todo o caso, os cidadãos 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 ao cidadão 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 ao cidadão 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 desse cidadão.

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. Nos termos do RGPD, os dados pessoais podem, na ausência de uma decisão de adequação, ser transferidos para um país terceiro se forem prestadas garantias adequadas em matéria de proteção de dados nos termos do artigo 46.º do RGPD ou, em situações específicas, se for cumprida uma das condições do artigo 49.º do RGPD (*por exemplo*, se o titular dos dados tiver consentido explicitamente a transferência). As organizações norte-americanas aderentes ao QPD UE-EUA asseguram uma proteção adequada dos dados pessoais, pelo que podem receber transferências de dados da UE com base no artigo 45.º do RGPD, sem terem de criar um instrumento de transferência nos termos do artigo 46.º ou de cumprir as condições previstas no artigo 49.º. Dado que o QPD UE-EUA contém normas específicas em matéria de informações sensíveis, esse tipo de informação (que, por exemplo, poderá ter de ser obtido por razões ligadas à 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 para o tratamento de dados sensíveis.

14. **Produtos farmacêuticos e medicinais**

a. Aplicação da legislação dos Estados-Membros da UE ou dos princípios

i. 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 aplicam-se aos dados após a transferência para os EUA. Os dados utilizados para investigação farmacêutica e outros fins deveriam, se possível, ser anonimizados.

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 norte-americana aderente ao QPD UE-EUA, a mesma pode utilizá-los para uma nova atividade de investigação científica se os princípios de aviso e escolha adequados tiverem sido 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 cidadão deu posteriormente o seu consentimento, deverá ser obtido um novo consentimento.

c. Retirada de um ensaio clínico

i. 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 desde 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

i. É permitido às empresas de dispositivos farmacêuticos e médicos fornecer dados pessoais provenientes de ensaios clínicos realizados na UE às entidades reguladoras nos Estados Unidos, para efeitos de regulamentação e supervisão. São permitidas transferências semelhantes a outras partes para além das entidades reguladoras, 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

i. Uma empresa de dispositivos farmacêuticos ou médicos não tem de aplicar os princípios no que diz respeito aos princípios de aviso, escolha, responsabilização 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

i. 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 só ele 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 Estados Unidos, ou seja, dados pessoais da UE nos termos do direito da UE, é abrangida pelos princípios.

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 aos dados pessoais de fontes disponíveis ao público. Estes princípios são igualmente aplicáveis aos dados pessoais recolhidos de registos públicos (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 responsabilização 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 responsabilização pela transferência ulterior à informação disponível ao público, exceto se o responsável europeu da transferência indicar que essa informação é objeto de restrições que requerem 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 QPD UE-EUA.

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 impostas 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. Em alternativa, as pessoas podem solicitar o acesso às suas informações à organização que inicialmente 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 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 essas comunicações estejam autorizadas nos termos da legislação aplicável.

b. As informações fornecidas nestes relatórios pelas organizações aderentes ao QPD UE-EUA, em conjunto com as informações divulgadas pelo setor das informações, a par de outras informações, podem contribuir para a reapreciação conjunta periódica do funcionamento do QPD UE-EUA 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 QPD UE-EUA são obrigadas a proceder à arbitragem de queixas, nos termos do princípio de recurso, aplicação e responsabilidade. A opção de arbitragem vinculativa descrita *infra* é aplicável a determinadas queixas «não resolvidas» relativas aos dados abrangidos pelo QPD UE-EUA 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 QPD UE-EUA.

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 violou as suas obrigações nos termos dos princípios para com o cidadão em causa, e se essa 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 QPD UE-EUA.

B. **Reparações disponíveis**

No âmbito desta opção de arbitragem, o Comité do Quadro de Privacidade de Dados UE-EUA (comité de arbitragem constituído por um ou três árbitros, conforme o acordado pelas partes) tem competência para aplicar medidas equitativas, não pecuniárias e específicas a cada cidadão (como acesso, correção, eliminação ou devolução dos dados do cidadão em questão) necessárias para reparar a violação dos princípios apenas no que se refere ao cidadão em questão. Estes são os únicos poderes do Comité do Quadro de Privacidade de Dados UE-EUA no que diz respeito às reparações. Aquando da ponderação das reparações, o Comité do Quadro de Privacidade de Dados UE-EUA deve ter em conta outras reparações que já tenham sido aplicadas por outros mecanismos no âmbito do QPD UE-EUA. 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 estabelecido na alínea d), subalínea i), do princípio suplementar sobre resolução de litígios e aplicação; 2) Utilizar o mecanismo de recurso independente previsto nos princípios, sem custos para o cidadão; e 3) Expor o problema ao *Department* por intermédio da APD e permitir que o *Department* envide os seus melhores esforços para resolver o problema nos prazos fixados na carta da *International Trade Administration* do *Department*, 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 uma decisão transitada em julgado relativa 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 APD: 1) tiver autoridade no âmbito do princípio suplementar sobre o papel das autoridades responsáveis pela proteção dos dados ou do princípio suplementar sobre dados relativos a recursos humanos; 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 devem ser vinculativas para todas as partes na arbitragem. Uma vez invocada a opção de arbitragem, ao cidadão abdica da possibilidade de requerer reparação por essa alegada violação noutra instância, com a exceção de que, se uma medida não pecuniária equitativa não permitir a reparação na íntegra da alegada violação, a invocação de arbitragem por parte da pessoa não exclui uma ação judicial de indemnização por perdas e danos.

([1]) *The Principles, Overview*, n.º 5.

E. **Controlo e execução**

Os cidadãos e as organizações aderentes poderão solicitar o controlo jurisdicional e a execução das decisões de arbitragem nos termos da legislação dos EUA ao abrigo da *Federal Arbitration Act* ([2]). Todos os casos deste tipo devem ser apresentados no tribunal federal distrital cuja competência territorial inclua o principal estabelecimento da organização aderente.

Esta opção de arbitragem destina-se a resolver litígios concretos 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**

Cabe às partes selecionar árbitros para o Comité do Quadro de Privacidade de Dados UE-EUA a partir da lista de árbitros *infra*.

Em conformidade com a legislação aplicável, o *Department* e a Comissão Europeia estabelecem uma lista de pelo menos dez 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 por um período de três anos, na ausência de circunstâncias excecionais ou de uma supressão por justa causa, renovável pelo *Department*, com notificação prévia à Comissão, por mandatos de três anos adicionais;

2) não devem receber quaisquer instruções de, nem estar associados a, qualquer parte, qualquer organização aderente, 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 Estados Unidos e ser peritos na legislação norte-americana relativa à privacidade, bem como ser especializados na legislação da UE em matéria de proteção de dados.

([2]) 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 da 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, a 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 decisão proferida, a menos que constate um dos motivos de recusa ou diferimento do reconhecimento ou da execução da decisão especificados na referida Convenção [de Nova Iorque]». Id., ponto 207; Além disso, o capítulo 2 determina 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., ponto 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., ponto 208; O capítulo 1, por sua vez, estabelece que «[u]ma disposição redigida num . contrato que evidencie uma transação que implique uma troca comercial com vista a resolver por arbitragem uma controvérsia decorrente desse contrato ou transação, ou a recusa em executar o mesmo parcialmente ou na íntegra, ou um acordo escrito com vista a submeter a arbitragem uma controvérsia existente decorrente desse contrato, transação ou recusa, será válido, irrevogável e executório, salvo disposição em contrário prevista pela lei ou pelo princípio de equidade para a revogação de um contrato». Id., ponto 2; Além disso, o capítulo 1 estabelece que «qualquer parte na arbitragem pode solicitar ao tribunal especificado um despacho que confirme a decisão e o tribunal deve emitir esse despacho, a menos que a decisão seja anulada, alterada ou corrigida, conforme prescrito nas secções 10 e 11 da [FAA]». Id., ponto 9;

G. **Procedimentos de arbitragem**

O *Department* e a Comissão acordaram, em conformidade com a legislação aplicável, na adoção de regras de arbitragem que regem os processos perante o Comité do Quadro de Privacidade de Dados UE-EUA ([3]). Caso as regras que regem os processos tenham de ser alteradas, o *Department* e a Comissão concordarão em alterar essas regras ou adotarão um conjunto diferente de procedimentos de arbitragem norte-americanos existentes e bem estabelecidos, consoante o caso, 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.

2. Devem ser aplicados procedimentos a fim de garantir que a mesma alegada violação invocada por um cidadão não é objeto de reparações ou procedimentos em duplicado.

3. A ação da FTC pode decorrer 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 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 deve realizar-se nos Estados Unidos e o cidadão pode optar pela participação por videoconferência ou telefone, que é prestada sem custos para o cidadão. Não deve ser requerida a participação presencial.

6. A língua utilizada na arbitragem deve ser o inglês, salvo acordo das partes em contrário. Mediante pedido fundamentado, e tomando em consideração se o cidadão é representado por um advogado, deve ser fornecida interpretação na audiência arbitral, bem como a tradução dos materiais de arbitragem, sem custos para o cidadão, a menos que o Comité do Quadro de Privacidade de Dados UE-EUA considere que, nas circunstâncias da arbitragem específica, tal conduziria a custos injustificados ou desproporcionados.

7. Os materiais apresentados aos árbitros devem ser tratados confidencialmente e a sua utilização limitada à arbitragem.

8. Os conteúdos específicos relativos ao cidadão podem ser autorizados, se necessário, devem ser tratados confidencialmente pelas partes e a sua utilização limitada à arbitragem.

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

([3]) O *Department* escolheu o *International Centre for Dispute Resolution* (ICDR), a divisão internacional da *American Arbitration Association* (AAA) (coletivamente, «ICDR-AAA»), para gerir as arbitragens nos termos do anexo I dos princípios e o fundo de arbitragem referido no mesmo anexo I dos princípios. Em 15 de setembro de 2017, o *Department* e a Comissão acordaram na adoção de um conjunto de regras de arbitragem para reger os processos de arbitragem vinculativos referidos no anexo I dos princípios, bem como um código de conduta destinado aos árbitros coerente com as normas éticas geralmente aceites aplicáveis aos árbitros comerciais e com o anexo I dos princípios. O *Department* e a Comissão acordaram em adaptar as regras de arbitragem e o código de conduta para refletir as atualizações efetuadas no âmbito do QPD UE-EUA, e o *Department* colaborará com o ICDR-AAA nessas atualizações.

H. **Custos**

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

O *Department*, em conformidade com a legislação aplicável, facilitará a manutenção de um fundo, para o qual as organizações participantes terão de contribuir, com base, em parte, na dimensão da organização, que cobrirá os custos de arbitragem, nomeadamente os honorários dos árbitros, até montantes máximos («limites máximos»). O fundo deve ser gerido por um terceiro, que regularmente apresentará ao *Department* informações sobre o funcionamento do fundo. O *Department* colaborará com o terceiro para analisar periodicamente o funcionamento do fundo, em especial a necessidade de ajustar o montante das contribuições ou dos limites máximos, e analisarão, entre outros elementos, o número de arbitragens, bem como os respetivos custos e calendarização, com o entendimento de que não será imposto um encargo financeiro excessivo sobre as organizações participantes. O *Department* notificará a Comissão do resultado dessas análises com o terceiro e fornecerá à Comissão uma notificação prévia de quaisquer ajustamentos do montante das contribuições. Os honorários dos advogados não são abrangidos pela presente disposição nem por qualquer fundo nos termos da presente disposição.

ANEXO II

UNITED STATES DEPARTMENT OF COMMERCE
Secretary of Commerce
Washington, D.C. 20230

6 de julho de 2023

Didier Reynders
Comissário da Justiça
Comissão Europeia
Rue de la Loi/ Westraat 200
1049 Bruxelas
Bélgica

Senhor Comissário,

Em nome dos Estados Unidos, tenho o prazer de transmitir um pacote de materiais relativo ao Quadro de Privacidade de Dados UE-EUA que, combinado com o *Executive Order 14086* intitulado «Enhancing Safeguards for United States Signals Intelligence Activities» e com o título 28, parte 201, do CFR que altera os regulamentos do *Department of Justice* para criar o *Data Protection Review Court*, reflete negociações importantes e exaustivas para reforçar a proteção da privacidade e das liberdades cívicas. Estas negociações resultaram em novas garantias para assegurar que as atividades de informação de origem eletromagnética dos EUA sejam necessárias e proporcionais à consecução dos objetivos de segurança nacional fixados e num novo mecanismo para que os cidadãos da União Europeia possam obter reparação se considerarem que são ilegalmente visados por atividades de informação de origem eletromagnética, o que, em conjunto, assegurará a privacidade dos dados pessoais da UE. O Quadro de Privacidade de Dados UE-EUA será a base de uma economia digital inclusiva e competitiva. Devemos estar ambos orgulhosos das melhorias refletidas nesse quadro, que reforçarão a proteção da privacidade em todo o mundo. Este pacote, a par do decreto executivo, dos regulamentos e de outros materiais acessíveis a partir de fontes públicas, constitui uma base muito sólida para uma nova verificação de adequação por parte da Comissão Europeia ([1]).

Em anexo, figuram os seguintes materiais:

— os princípios do Quadro de Privacidade de Dados UE-EUA, em especial os princípios suplementares (coletivamente, «os princípios») e o anexo I dos princípios (*ou seja*, um anexo que estabelece as condições segundo as quais as organizações do Quadro de Privacidade de Dados são obrigadas a proceder à arbitragem de determinadas queixas não resolvidas relativas a dados pessoais abrangidos pelos princípios),

— uma carta da *International Trade Administration* do *Department*, que administra o programa do Quadro de Privacidade de Dados, descrevendo os compromissos que o *Department* assumiu para assegurar que o Quadro de Privacidade de Dados UE-EUA funciona de forma eficaz,

— Um ofício da *Federal Trade Commission* que descreve a sua aplicação aos princípios;

— Um ofício do *Department of Transportation* que descreve a sua aplicação aos princípios;

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

— Um ofício elaborado 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.

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

O pacote completo do Quadro de Privacidade de Dados UE-EUA será publicado no sítio Web do Quadro de Privacidade de Dados do *Department*, ao passo que os princípios e o anexo I dos princípios serão aplicáveis na data de entrada em vigor da decisão de adequação da Comissão Europeia.

Posso garantir que os Estados Unidos da América encaram estes compromissos com seriedade. Aguardamos com expectativa a possibilidade de trabalhar convosco na implementação do Quadro de Privacidade de Dados UE-EUA e no início da próxima fase deste projeto conjunto.

Queira aceitar a expressão da minha mais elevada consideração,

Gina M. Raimondo

ANEXO III

UNITED STATES DEPARTMENT OF COMMERCE
International Trade Administration
Washington, D C 20230

12 de dezembro de 2022

Didier Reynders
Comissário da Justiça
Comissão Europeia
Rue de la Loi/Westraat 200
1049 Bruxelas
Bélgica

Senhor Comissário,

Em nome da *International Trade Administration* (ITA), tenho o prazer de descrever os compromissos assumidos pelo *Department of Commerce* («Department») para assegurar a proteção dos dados pessoais através da sua administração e supervisão no âmbito do programa do Quadro de Privacidade de Dados. A conclusão do Quadro de Privacidade de Dados UE-EUA («QPD UE-EUA») é uma conquista importante para a privacidade e para as empresas de ambos os lados do Atlântico, uma vez que proporcionará aos cidadãos da UE a confiança de que os seus dados são protegidos e de que têm à sua disposição vias de recurso para resolver os problemas relacionados com os seus dados, e permitirá que milhares de empresas continuem a investir e de outro modo a estabelecer relações comerciais através do Atlântico, em benefício das nossas respetivas economias e cidadãos. O QPD UE-EUA reflete anos de trabalho árduo e colaboração com Vossa Excelência e com os seus colegas da Comissão Europeia («Comissão»). Aguardamos com expectativa a oportunidade de continuar a trabalhar com a Comissão a fim de assegurar o funcionamento eficaz desta colaboração.

O novo QPD UE-EUA permitirá vários benefícios significativos tanto para os cidadãos 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 transferidos para os Estados Unidos. Determina que as organizações norte-americanas aderentes desenvolvam uma política em matéria de proteção da privacidade conforme; que assumam publicamente o compromisso de cumprir os «princípios do Quadro de Privacidade de Dados UE-EUA», em especial os princípios suplementares (coletivamente, «os princípios»), e o anexo I dos princípios (*ou seja*, um anexo que estabelece as condições segundo as quais as organizações do QPD UE-EUA são obrigadas a proceder à arbitragem de determinadas queixas não resolvidas relativas a dados pessoais abrangidos pelos princípios), por forma a que o compromisso se torne executório nos termos do direito dos EUA ([1]), que renovem anualmente a certificação de conformidade junto do *Department*, que disponibilizem a resolução independente de litígios gratuita aos cidadãos da UE e que estejam sujeitas à autoridade de investigação e de aplicação da lei de um organismo oficial norte-americano referido nos princípios [*por exemplo*, a *Federal Trade Commission* (FTC) e o *Department of Transportation* (DOT)] ou de um organismo oficial norte-americano referido num futuro anexo dos princípios. Embora a decisão de autocertificação de uma empresa seja voluntária, quando uma organização adere publicamente ao QPD UE-EUA, o seu compromisso é executório nos termos do direito dos EUA, pela FTC, pelo DOT ou por outro organismo oficial norte-americano, em função do organismo competente no que diz respeito à organização participante. Em segundo

([1]) As organizações que autocertificaram o seu compromisso de cumprir os princípios do Escudo de Proteção da Privacidade UE-EUA e que pretendam usufruir dos benefícios da participação no QPD UE-EUA devem cumprir os «princípios do Quadro de Privacidade de Dados UE-EUA». Este compromisso de cumprir os «princípios do Quadro de Privacidade de Dados UE-EUA» deve refletir-se nas políticas de privacidade das organizações participantes o mais rapidamente possível e, em todo o caso, o mais tardar três meses após a data de entrada em vigor dos «princípios do Quadro de Privacidade de Dados UE-EUA». (*Ver* subponto e do princípio suplementar sobre autocertificação).

lugar, o QPD UE-EUA permitirá que as empresas dos Estados Unidos, incluindo filiais de empresas europeias situadas nos Estados Unidos, recebam dados pessoais da União Europeia com vista a facilitar os fluxos de dados subjacentes ao comércio transatlântico. Os fluxos de dados entre os Estados Unidos e a União Europeia são os maiores do mundo e sustentam a relação económica entre os EUA e a UE no valor de 7,1 biliões de USD, que suporta 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. 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 *Department* está empenhado em trabalhar em estreita colaboração e de forma produtiva com os seus homólogos da UE para administrar e supervisionar eficazmente o programa do Quadro de Privacidade de Dados. Este compromisso reflete-se no desenvolvimento e no aperfeiçoamento contínuo, por parte do *Department*, de uma diversidade de recursos para assistir as organizações no processo de autocertificação, na criação de um sítio Web para fornecer informações específicas às partes interessadas, na colaboração com a Comissão e com as autoridades europeias de proteção de dados (APD) para elaborar orientações que clarifiquem elementos importantes do QPD UE-EUA, na sensibilização para facilitar uma maior compreensão das obrigações de proteção de dados das organizações e na supervisão e controlo do cumprimento dos requisitos do programa pelas organizações.

A nossa cooperação contínua com os nossos estimados homólogos da UE permitirá ao *Department* assegurar que o QPD UE-EUA funciona de forma eficaz. O Governo dos Estados Unidos tem uma longa história de colaboração com a Comissão para promover princípios comuns de proteção de dados, colmatando as diferenças entre as nossas respetivas abordagens jurídicas e promovendo simultaneamente o comércio e o crescimento económico na União Europeia e nos Estados Unidos. Entendemos que o QPD UE-EUA, que é um exemplo desta cooperação, permitirá que a Comissão emita uma nova decisão de adequação que permitirá às organizações utilizar o QPD UE-EUA para transferir dados pessoais da União Europeia para os Estados Unidos em conformidade com o direito da UE.

Administração e supervisão do programa do Quadro de Privacidade de Dados pelo *Department of Commerce*

O *Department* está firmemente empenhado na administração e supervisão eficazes do programa do Quadro de Privacidade de Dados e envidará os esforços oportunos e afetará os recursos adequados para assegurar esse resultado. O *Department* manterá e disponibilizará ao público uma lista oficial das organizações norte-americanas que declararam a sua adesão junto do *Department*, bem como o seu compromisso de aderir aos princípios («lista do Quadro de Privacidade de Dados»), que será atualizada com base nas declarações de renovação da certificação anual apresentadas pelas organizações participantes e mediante a supressão das organizações quando estas se retirem voluntariamente, não efetuem a renovação da certificação anual de acordo com os procedimentos do *Department* ou não cumpram os princípios de forma persistente. O *Department* também manterá e disponibilizará ao público um registo oficial das organizações norte-americanas que foram suprimidas da lista do Quadro de Privacidade de Dados e indicará o motivo pelo qual cada organização foi suprimida. A lista e o registo oficiais referidos acima permanecerão disponíveis ao público no sítio Web do Quadro de Privacidade de Dados do *Department*. O sítio Web do Quadro de Privacidade de Dados incluirá uma explicação bem visível indicando que qualquer organização suprimida da lista do Quadro de Privacidade de Dados deve deixar de alegar que participa ou cumpre o QPD UE-EUA e que pode receber informações pessoais nos termos do QPD UE-EUA. No entanto, enquanto conservar essas informações, essa organização deve continuar a aplicar os princípios às informações pessoais que recebeu enquanto participou no QPD UE-EUA. O *Department*, no cumprimento do seu compromisso global e contínuo para com a administração e supervisão eficazes do programa do Quadro de Privacidade de Dados, compromete-se especificamente a efetuar o seguinte:

Verificar os requisitos de autocertificação

— O *Department*, antes de concluir a autocertificação inicial ou a renovação da certificação anual de uma organização (coletivamente, «autocertificação») e de inscrever ou manter uma organização na lista do Quadro de Privacidade de Dados, verificará se a organização cumpriu, no mínimo, os requisitos pertinentes estabelecidos no princípio suplementar sobre autocertificação relativamente às informações que uma organização deve fornecer na sua declaração de autocertificação ao *Department* e se forneceu, em tempo oportuno, uma política de privacidade pertinente que informa os cidadãos sobre todos os 13 elementos referidos e estabelecidos no princípio de aviso. O *Department* verificará se a organização:

— indicou a organização que está a apresentar a sua declaração de autocertificação, bem como quaisquer entidades norte-americanas ou filiais norte-americanas da organização que se autocertifica que também estão a aderir aos princípios que a organização pretende que sejam abrangidas pela sua autocertificação,

— apresentou as informações de contacto necessárias da organização (*por exemplo*, as informações de contacto de pessoas específicas e/ou de gabinetes na organização que se autocertifica responsáveis pelo tratamento das queixas, dos pedidos de acesso e de quaisquer outras questões decorrentes do QPD UE-EUA),

— descreveu a(s) finalidade(s) para a(s) qual(ais) a organização recolherá e utilizará as informações pessoais recebidas da União Europeia,

— indicou que informações pessoais receberá da União Europeia com base no QPD UE-EUA e, por conseguinte, abrangidas pela sua autocertificação,

— se a organização tiver um sítio Web público, forneceu o endereço URL em que figura a política de privacidade pertinente facilmente acessível nesse sítio Web ou, se a organização não tiver um sítio Web público, forneceu ao *Department* uma cópia da política de privacidade pertinente e indicou em que local essa política de privacidade está disponível para consulta pelos cidadãos afetados (ou seja, os empregados afetados se a política de privacidade pertinente for uma política de privacidade dos recursos humanos ou o público se a política de privacidade pertinente não for uma política de privacidade dos recursos humanos),

— incluiu na sua política de privacidade pertinente, no momento oportuno (ou seja, inicialmente apenas o projeto de política de privacidade fornecido em conjunto com a declaração, se essa declaração for uma autocertificação inicial; caso contrário, a política de privacidade final e, se for caso disso, publicada), uma declaração de que adere aos princípios e uma ligação ou o endereço URL do sítio Web do Quadro de Privacidade de Dados do *Department* (por exemplo, a página principal ou a página Web da lista do Quadro de Privacidade de Dados),

— incluiu na sua política de privacidade pertinente, no momento oportuno, todos os outros 12 elementos enumerados no princípio da comunicação (por exemplo, a possibilidade de, em determinadas condições, o cidadão da UE afetado invocar a arbitragem vinculativa; 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 a sua responsabilidade em caso de transferências ulteriores para terceiros);

— 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 regulem a privacidade (e que se encontram referidos nos princípios ou num futuro anexo dos princípios);

— identificou qualquer programa relativo à privacidade em que a organização participe;

— indicou que o método pertinente (*ou seja*, os procedimentos de acompanhamento que deve fornecer) para verificar a sua conformidade com os princípios é a «autoavaliação» (*ou seja*, a verificação interna) ou a «verificação de conformidade externa» (ou seja, a verificação por terceiros) e, caso tenha indicado o método pertinente como sendo a verificação de conformidade externa, indicou também o terceiro que concluiu essa verificação,

— indicou o mecanismo de recurso independente apropriado disponível para resolver as queixas apresentadas nos termos dos princípios e proporcionar vias de recurso adequadas e gratuitas ao cidadão afetado:

  — se a organização selecionou um mecanismo de recurso independente fornecido por um organismo de resolução alternativa de litígios do setor privado, incluiu na sua política de privacidade pertinente uma ligação ou o endereço URL do sítio Web pertinente ou do formulário de apresentação de queixas do mecanismo disponível para investigar queixas não resolvidas apresentadas nos termos dos princípios,

  — Se a organização for obrigada (*ou seja*, no que respeita aos dados relativos aos recursos humanos transferidos da União Europeia no contexto da relação laboral) ou tiver optado por cooperar com as APD competentes na investigação e resolução das queixas apresentadas nos termos dos princípios, declarou o seu compromisso de cooperação com as APD e a agir em conformidade com as orientações das APD para tomar medidas específicas a fim de cumprir os princípios;

— o *Department* verificará ainda se a declaração de autocertificação da organização é coerente com a(s) sua(s) política(s) de privacidade pertinente(s). Quando uma organização que se autocertifica pretende abranger qualquer uma das suas entidades norte-americanas ou filiais norte-americanas que tenham políticas de privacidade separadas e pertinentes, o *Department* também analisará as políticas de privacidade pertinentes dessas entidades ou filiais abrangidas para assegurar que incluem todos os elementos exigidos estabelecidos no princípio de aviso,

— o *Department* colaborará com os organismos oficiais (*por exemplo*, a FTC e o DOT) para verificar se as organizações estão subordinadas à competência do organismo oficial competente indicado nas suas declarações de autocertificação, sempre que o *Department* tenha razões para duvidar de que estão subordinadas a essa competência,

— o *Department* colaborará com os organismos de resolução alternativa de litígios do setor privado para verificar se as organizações estão efetivamente registadas no mecanismo de recurso independente indicado nas suas declarações de autocertificação; além disso colaborará com esses organismos para verificar se as organizações estão efetivamente registadas para a verificação de conformidade externa indicada nas suas declarações de autocertificação, sempre que esses organismos possam oferecer ambos os tipos de serviços,

— o *Department* colaborará com o terceiro selecionado pelo *Department* para servir de depositário dos fundos obtidos através da taxa do painel das APD (ou seja, a taxa anual destinada a cobrir os custos de funcionamento do painel das APD), para verificar se as organizações pagaram essa taxa relativa ao ano em causa, sempre que as organizações indiquem as APD como o mecanismo de recurso independente pertinente,

— o *Department* colaborará com o terceiro selecionado pelo *Department* para administrar as arbitragens nos termos do anexo I dos princípios e gerir o fundo de arbitragem referido no mesmo anexo I dos princípios, a fim de verificar se as organizações contribuíram para esse fundo de arbitragem,

— se o *Department* identificar quaisquer problemas durante a sua análise das declarações de autocertificação das organizações, informá-las-á de que devem resolver todos esses problemas dentro do prazo adequado fixado pelo *Department* ([2]). O *Department* também as informará de que a falta de resposta dentro dos prazos fixados pelo *Department* ou a não conclusão da sua autocertificação de acordo com os procedimentos do *Department* conduzirá a que essas autocertificações sejam consideradas abandonadas e que quaisquer declarações falsas sobre a participação de uma organização no QPD UE-EUA ou sobre a sua conformidade com o mesmo pode ser objeto de medidas coercivas por parte da FTC, do DOT ou de outro organismo governamental competente. O *Department* informará as organizações através dos meios de contacto fornecidos por estas ao *Department*.

Facilitar a cooperação com os organismos de resolução alternativa de litígios que prestam serviços relacionados com os princípios

— o *Department* colaborará com os organismos de resolução alternativa de litígios do setor privado que forneçam mecanismos de recurso independentes, disponíveis para investigar queixas não resolvidas apresentadas nos termos dos princípios, para verificar se cumprem, no mínimo, os requisitos estabelecidos no princípio suplementar sobre resolução de litígios e aplicação. O *Department* verificará se as organizações:

  — incluem informações nos seus sítios Web públicos relativas aos princípios e aos serviços que prestam no âmbito do QPD UE-EUA, que devem incluir: 1) informações sobre os requisitos dos princípios aplicáveis aos mecanismos de recurso independentes ou uma hiperligação para os mesmos; 2) uma hiperligação para o sítio Web relativo ao Quadro de Privacidade de Dados do *Department*; 3) um esclarecimento de que os seus serviços de resolução de litígios no âmbito do QPD UE-EUA são gratuitos para os cidadãos; 4) uma descrição de como é possível apresentar uma queixa relacionada com os princípios; 5) o prazo para o tratamento das queixas relacionadas com os princípios; e 6), uma descrição do conjunto de possíveis vias de recurso. O *Department* notificará atempadamente os organismos das alterações significativas à supervisão e administração do programa do Quadro de Privacidade de Dados por parte do *Department*, sempre que essas alterações estejam iminentes ou já tenham sido efetuadas e sejam pertinentes para o papel que os organismos desempenham no âmbito do QPD UE-EUA,

([2]) *Por exemplo*, no que diz respeito à renovação da certificação, espera-se que as organizações resolvam todos esses problemas no prazo de 45 dias; sob reserva da fixação de um prazo diferente e adequado pelo *Department*.

— publicam um relatório anual com estatísticas agregadas relativas aos seus serviços de resolução de litígios, que deve incluir: 1) o número total de queixas relacionadas com os princípios 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. O *Department* fornecerá aos organismos orientações específicas e complementares sobre as informações que devem incluir nesses relatórios anuais elaborados tendo em conta esses requisitos (por exemplo, referindo os critérios específicos que uma queixa deve satisfazer para ser considerada uma queixa relacionada com os princípios para efeitos do relatório anual), bem como identificando outros tipos de informações que estas devem incluir (por exemplo, se o organismo também presta um serviço de verificação relacionado com os princípios, uma descrição da forma como o organismo evita quaisquer conflitos de interesses reais ou potenciais nas situações em que presta tanto serviços de verificação como serviços de resolução de litígios a uma organização). As orientações adicionais fornecidas pelo *Department* também especificarão a data em que os relatórios anuais dos organismos devem ser publicados para o período de apresentação de relatórios em causa.

Acompanhamento das organizações que pretendem ser suprimidas da lista do Quadro de Privacidade de Dados ou que tenham sido suprimidas da mesma

— Se uma organização pretender retirar-se do QPD UE-EUA, o *Department* exigirá que a organização suprima de qualquer política de privacidade pertinente quaisquer referências ao QPD UE-EUA que sugiram que esta continua a participar no QPD UE-EUA e que recebe dados pessoais no âmbito do QPD UE-EUA (*ver* a descrição do compromisso do *Department* de procurar falsas alegações de participação). O *Department* exigirá ainda que a organização preencha e lhe envie um questionário adequado para verificar:

  — a sua intenção de se retirar,

  — qual das seguintes ações empreenderá relativamente aos dados pessoais que recebeu com base no QPD UE-EUA enquanto participou no QPD UE-EUA: a) conservar esses dados, continuar a aplicar os princípios a esses dados e confirmar anualmente ao *Department* o seu compromisso de aplicar os princípios a esses dados; b) conservar esses dados e assegurar uma proteção «adequada» desses dados através de outros meios autorizados; ou c) devolver ou eliminar todos esses dados até uma determinada data; e

  — que pessoa, no seio da organização, servirá como ponto de contacto permanente para as questões relacionadas com os princípios.

— se uma organização optar por: a), conforme descrito imediatamente acima, o *Department* também exigirá que a organização preencha e apresente ao *Department* todos os anos após a sua retirada (*ou seja*, até ao primeiro aniversário da sua retirada, bem como até cada aniversário subsequente, salvo se e até que a organização assegure uma proteção «adequada» desses dados através de outros meios autorizados ou devolva ou elimine todos esses dados e notifique o *Department* desta ação) um questionário adequado para verificar o que fez com esses dados pessoais, o que fará com quaisquer desses dados pessoais que continua a conservar e que pessoa, no seio da organização, servirá como ponto de contacto permanente para as questões relacionadas com os princípios,

— se uma organização deixar que a sua autocertificação caduque (*ou seja*, não efetuou a sua renovação da certificação anual da sua adesão aos princípios nem foi retirada da lista do Quadro de Privacidade de Dados por qualquer outro motivo, como a retirada), o *Department* ordenar-lhe-á que preencha e apresente ao *Department* um questionário adequado para verificar se pretende retirar-se ou renovar a certificação:

  — e, se a organização pretender retirar-se, verificar novamente o que a organização fará com os dados pessoais que recebeu com base no QPD UE-EUA enquanto participou no QPD UE-EUA (*ver* a descrição anterior em relação aos elementos que uma organização deve verificar se pretender retirar-se),

  — e, se organização pretender renovar a certificação, verificar novamente se a organização, durante o tempo em que o seu estatuto de certificação esteve caducado, aplicou os princípios aos dados pessoais recebidos no âmbito do QPD UE-EUA e esclarecer que medidas a organização tomará para resolver as questões pendentes que conduziram ao retardamento da sua renovação da certificação.

— se uma organização for suprimida da lista do Quadro de Privacidade de Dados por qualquer um dos seguintes motivos: a) retirada do QPD UE-EUA, b) não realização da renovação da certificação anual da sua adesão aos princípios (*ou seja*, ou iniciou, mas não concluiu o processo de renovação da certificação anual em tempo útil ou não chegou a iniciar o processo de renovação da certificação anual), ou c) «incumprimento persistente», o *Department* enviará uma notificação ao(s) contacto(s) indicado(s) na declaração de autocertificação da organização, especificando o motivo da supressão e explicando que esta deve deixar de fazer quaisquer alegações explícitas ou implícitas de que participa ou cumpre o QPD UE-EUA e que pode receber dados pessoais nos termos do QPD UE-EUA. A notificação, que também pode incluir outro conteúdo adaptado ao motivo da supressão, indicará que as organizações que alegam falsamente a sua participação ou conformidade com o QPD UE-EUA, em especial as que afirmam estar a participar no QPD UE-EUA depois de terem sido suprimidas da lista do Quadro de Privacidade de Dados, podem ser objeto de medidas coercivas por parte da FTC, do DOT ou de outro organismo governamental competente.

Identificação e tratamento das falsas alegações de adesão

— numa base contínua, sempre que uma organização: a) deixe de participar no QPD UE-EUA, b) não renove a certificação anual da sua adesão aos princípios (*ou seja*, ou iniciou, mas não concluiu o processo de renovação da certificação anual em tempo útil ou não chegou a iniciar o processo de renovação da certificação anual), c) seja excluída como participante no QPD UE-EUA, nomeadamente devido a «incumprimento persistente», ou d) não efetue uma autocertificação inicial da sua adesão aos princípios (*ou seja*, iniciou, mas não concluiu o processo de autocertificação inicial em tempo útil), o *Department* tomará, sistematicamente, medidas para verificar se qualquer política de privacidade pertinente publicada pela organização não contém referências ao QPD UE-EUA que sugiram que a organização participa no QPD UE-EUA e que pode receber dados pessoais nos termos do QPD UE-EUA. Sempre que o *Department* encontrar tais referências, informará a organização de que, consoante o caso, submeterá a questão ao serviço competente para a aplicação de potenciais medidas coercivas se a organização continuar a alegar falsamente a sua participação no QPD UE-EUA. O *Department* informará a organização através dos meios de contacto fornecidos pela organização ao *Department* ou, se necessário, através de outros meios adequados. Se a organização não suprimir as referências nem autocertificar a sua conformidade com o QPD UE-EUA de acordo com os procedimentos do *Department*, este submeterá sistematicamente a questão à FTC, ao DOT ou a outro serviço de execução competente, podendo também tomar outras medidas adequadas para assegurar a utilização correta da marca de certificação do QPD UE-EUA,

— o *Department* envidará outros esforços para identificar falsas alegações de participação no QPD UE-EUA e a utilização indevida da marca de certificação do QPD UE-EUA, nomeadamente por organizações que, ao contrário das organizações descritas imediatamente acima, nunca iniciaram o processo de autocertificação (*por exemplo*, efetuando pesquisas adequadas na Internet para identificar referências ao QPD UE-EUA nas políticas de privacidade das organizações). Se, através destes esforços, o *Department* identificar falsas alegações de participação no QPD UE-EUA e utilizações indevidas da marca de certificação do QPD UE-EUA, este informará a organização de que, consoante o caso, submeterá a questão ao serviço competente para a aplicação de potenciais medidas coercivas, se a organização continuar a alegar falsamente a sua participação no QPD UE-EUA. O *Department* informará a organização através dos meios de contacto, caso existam, fornecidos pela organização ao *Department* ou, se necessário, através de outros meios adequados. Se a organização não suprimir as referências nem autocertificar a sua conformidade com o QPD UE-EUA de acordo com os procedimentos do *Department*, este submeterá sistematicamente a questão à FTC, ao DOT ou a outro serviço de execução competente, podendo também tomar outras medidas adequadas para assegurar a utilização correta da marca de certificação do QPD UE-EUA,

— o *Department* analisará e responderá prontamente a queixas específicas e não abusivas sobre alegações falsas de participação no QPD UE-EUA que o *Department* receba (*por exemplo*, queixas recebidas das APD, dos mecanismos de recurso independentes fornecidos por organismos de resolução alternativa de litígios do setor privado, dos titulares dos dados, das empresas da UE e dos EUA e de outros tipos de terceiros), e

— O *Department of Commerce* pode tomar outras medidas corretivas adequadas. As declarações falsas prestadas ao *Department* poderão ser objeto de recurso ao abrigo da False Statements Act (18 USC § 1001).

Realizará oficiosamente verificações de conformidade sistemáticas, bem como avaliações do programa do Quadro de Privacidade de Dados

— numa base contínua, o *Department* envidará esforços para controlar o cumprimento efetivo por parte das organizações do QPD UE-EUA, para identificar questões que possam justificar a aplicação de medidas de acompanhamento. Em especial, o *Department* efetuará, sistematicamente, verificações aleatórias de rotina a organizações do QPD UE-EUA selecionadas de modo casual, bem como verificações aleatórias *ad hoc* a organizações específicas do QPD UE-EUA quando forem identificadas potenciais deficiências de cumprimento (por exemplo, potenciais deficiências de cumprimento dadas a conhecer ao *Department* por terceiros) para verificar se: a) o ponto de contacto responsável ou os pontos de contacto responsáveis pelo tratamento de queixas, pedidos de acesso e outras questões decorrentes do QPD UE-EUA estão disponíveis; b) se for caso disso, a política de privacidade da organização está facilmente acessível para consulta pelo público, tanto no sítio Web público da organização como através de uma ligação constante da lista do Quadro de Privacidade de Dados; c) a política de privacidade da organização continua a cumprir os requisitos de autocertificação descritos nos princípios; e d) o mecanismo independente de resolução de litígios indicado pela organização está disponível para responder às queixas apresentadas no âmbito do QPD UE-EUA. O *Department* também acompanhará ativamente as notícias que forneçam provas credíveis de incumprimento por parte das organizações do QPD UE-EUA,

— no âmbito da verificação de conformidade, o *Department* exigirá às organizações do QPD UE-EUA que preencham e apresentem ao *Department* um questionário pormenorizado, sempre que: a) o *Department* tenha recebido queixas válidas específicas sobre a conformidade da organização com os princípios, b) a organização não responda de forma válida aos pedidos de informações apresentados pelo *Department* sobre o QPD UE-EUA, ou c) existam provas credíveis de que a organização não cumpre os seus compromissos previstos no âmbito do QPD UE-EUA. Sempre que o *Department* enviar esse questionário pormenorizado a uma organização e esta não lhe der resposta satisfatória, o *Department* informará a organização de que, se não receber uma resposta atempada e satisfatória da organização, submeterá, consoante o caso, a questão ao serviço competente para a aplicação de potenciais medidas coercivas. O *Department* informará a organização através dos meios de contacto fornecidos pela organização ao *Department* ou, se necessário, através de outros meios adequados. Se a organização não apresentar uma resposta atempada e satisfatória, o *Department* submeterá, sistematicamente, a questão à FTC, ao DOT ou a outro serviço de execução competente, podendo também tomar outras medidas adequadas para assegurar o cumprimento. Sempre que adequado, o *Department* consultará as autoridades competentes em matéria de proteção dos dados sobre as referidas verificações de conformidade; e

— o *Department* avaliará periodicamente a administração e a supervisão do programa do Quadro de Privacidade de Dados para assegurar que os seus esforços de acompanhamento, incluindo quaisquer esforços empreendidos através da utilização de ferramentas de pesquisa (*por exemplo*, para verificar a existência de ligações obsoletas para as políticas de privacidade das organizações do QPD UE-EUA), são adequados para resolver os problemas existentes e quaisquer novos problemas à medida que estes surjam.

Adaptará o sítio Web do Quadro de Privacidade de Dados a públicos específicos

O *Department* adaptará o sítio Web do Quadro de Privacidade de Dados para que seja orientado para os seguintes públicos-alvo: cidadãos da UE, empresas da UE, empresas dos EUA e APD. A inclusão de material destinado diretamente aos cidadãos da UE e às empresas da UE permite facilitar a transparência de várias formas. No que se refere aos cidadãos da UE, o sítio Web explicará claramente: 1) os direitos que o QPD UE-EUA 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 QPD UE-EUA. No respeitante às empresas da UE, facilitará a verificação dos seguintes elementos: 1) se uma organização aderiu ao QPD UE-EUA; 2) o tipo de informações abrangidas pela autocertificação de adesão de uma organização ao QPD UE-EUA; 3) a política de privacidade aplicável às informações abrangidas; e 4) o método utilizado pela organização para verificar a sua adesão aos princípios. No que se refere aos cidadãos da UE, explicará claramente: 1) os benefícios da adesão ao QPD UE-EUA; 2) as modalidades de adesão ao QPD UE-EUA, bem como as modalidades de renovação da certificação e de retirada do QPD UE-EUA; e 3) de que forma os Estados Unidos administram e aplicam o QPD UE-EUA. A inclusão de material diretamente dirigido às APD (por exemplo, informações sobre o ponto de contacto específico do *Department* para as APD e uma ligação para o conteúdo relacionado com os princípios no sítio Web da FTC) facilitará a cooperação e a transparência. O *Department* também trabalhará numa base *ad hoc* com a Comissão e com o Comité Europeu para a Proteção de Dados (CEPD) para desenvolver material atual adicional (*por exemplo*, respostas a perguntas mais frequentes) para utilização no sítio Web do Quadro de Privacidade de Dados, sempre que essa informação facilite a administração e a supervisão eficientes do programa do Quadro de Privacidade de Dados.

Facilitar a cooperação com as APD

Para aumentar as oportunidades de cooperação com as APD, o *Department* manterá um ponto de contacto dedicado no *Department* que estabelecerá contactos com as APD. Nos casos em que a APD considere que uma organização que aderiu ao QPD UE-EUA não cumpre os princípios, designadamente na sequência de uma queixa de um cidadão da UE, a APD tem competência para contactar o ponto de contacto dedicado do *Department* para solicitar uma reapreciação mais pormenorizada da organização. O *Department* envidará os seus melhores esforços para facilitar a resolução da queixa junto da organização aderente ao QPD UE-EUA. No prazo de 90 dias após a receção da queixa, o *Department* apresentará uma atualização à APD. O ponto de contacto dedicado receberá igualmente consultas relativas a organizações que aleguem falsamente a sua adesão ao QPD UE-EUA. O ponto de contacto dedicado acompanhará todas as queixas submetidas pelas APD ao *Department* e este último apresentará, na reapreciação anual descrita *infra*, um relatório de análise agregada das queixas que recebe todos os anos. O ponto de contacto dedicado assistirá as APD na pesquisa de informações relacionadas com a autocertificação de uma organização específica ou com a anterior participação no programa e o ponto de contacto dedicado responderá às questões da APD sobre a aplicação de requisitos específicos do QPD UE-EUA. O *Department* também cooperará com a Comissão e com o CEPD em aspetos processuais e administrativos do painel das APD, nomeadamente o estabelecimento de procedimentos adequados para a distribuição dos fundos obtidos através da taxa do painel das APD. Temos presente que a Comissão colaborará com o *Department* para facilitar a resolução de quaisquer questões que possam surgir relativamente a esses procedimentos. Em segundo lugar, o *Department* fornecerá às APD o material relativo ao QPD UE-EUA 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 QPD UE-EUA 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.

Cumprir os seus compromissos nos termos do anexo I dos princípios

O *Department* cumprirá os seus compromissos nos termos do anexo I dos princípios, designadamente a manutenção de uma lista de árbitros selecionados pela Comissão com base na independência, na integridade e em conhecimentos especializados, e apoiará, consoante o caso, o terceiro selecionado pelo *Department* para administrar as arbitragens nos termos do anexo I dos princípios e gerir o fundo de arbitragem referido no mesmo anexo I dos princípios ([3]). O *Department* colaborará com o terceiro para, entre outros aspetos, verificar se este mantém um sítio Web com orientações sobre o processo de arbitragem, nomeadamente: 1) como iniciar o processo e apresentar documentos; 2) a lista de árbitros mantida pelo *Department* e como selecionar árbitros dessa lista; 3) os procedimentos de arbitragem aplicáveis e o código de conduta destinado aos árbitros aplicável e adotado pelo *Department* e pela Comissão ([4]); e 4) a cobrança e o pagamento dos honorários dos árbitros. Além disso, o *Department* colaborará com o terceiro para analisar periodicamente o funcionamento do fundo de arbitragem, em especial a necessidade de ajustar o montante das contribuições ou os limites máximos (*ou seja*, os montantes máximos) dos custos de arbitragem, e terá em conta, entre outros elementos, o número de arbitragens, bem como os respetivos custos e calendarização, com o entendimento de que não será imposto um encargo financeiro excessivo sobre as organizações do QPD UE-EUA. O *Department* notificará a Comissão do resultado dessas análises com o terceiro e fornecerá à Comissão uma notificação prévia de quaisquer ajustamentos do montante das contribuições.

Efetuar análises conjuntas do funcionamento do QPD UE-EUA

O *Department* e outras agências, consoante o caso, realizarão reuniões periódicas com a Comissão, com as APD interessadas e com os representantes adequados do CEPD, nas quais o *Department* fornecerá informações atualizadas sobre o QPD UE-EUA. As reuniões incluirão a discussão de questões atuais relacionadas com o funcionamento, a implementação, a supervisão e a aplicação do programa do Quadro de Privacidade de Dados. As reuniões podem, consoante o caso, incluir a discussão de temas conexos, como outros mecanismos de transferência de dados que beneficiam das garantias do QPD UE-EUA.

([3]) O *Department* escolheu o *International Centre for Dispute Resolution* (ICDR), a divisão internacional da *American Arbitration Association* (AAA) (coletivamente, «ICDR-AAA»), para administrar as arbitragens nos termos do anexo I dos princípios e gerir o fundo de arbitragem referido no mesmo anexo I dos princípios.

([4]) Em 15 de setembro de 2017, o *Department* e a Comissão acordaram na adoção de um conjunto de regras de arbitragem para reger os processos de arbitragem vinculativos referidos no anexo I dos princípios, bem como um código de conduta destinado aos árbitros coerente com as normas éticas geralmente aceites aplicáveis aos árbitros comerciais e com o anexo I dos princípios. O *Department* e a Comissão acordaram em adaptar as regras de arbitragem e o código de conduta para refletir as atualizações efetuadas no âmbito do QPD UE-EUA, e o *Department* colaborará com o ICDR-AAA nessas atualizações.

Atualização da legislação

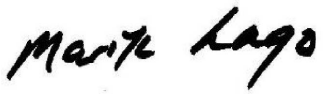
O *Department* deve efetuar todas as diligências razoáveis para informar a Comissão dos desenvolvimentos significativos da legislação nos Estados Unidos, desde que sejam pertinentes para o QPD UE-EUA em matéria de proteção da privacidade dos dados, e das limitações e salvaguardas aplicáveis ao acesso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

Acesso do Governo dos EUA aos dados pessoais

Os Estados Unidos emitiram o *Executive Order 14086* intitulado «Enhancing Safeguards for United States Signals Intelligence Activities» e o título 28, parte 201, do CFR que altera os regulamentos do *Department of Justice* para criar o *Data Protection Review Court* (DPRC), que proporciona uma proteção sólida dos dados pessoais no que diz respeito ao acesso do governo aos dados para fins de segurança nacional. A proteção prevista inclui o reforço das garantias em matéria de privacidade e liberdades cívicas para assegurar que as atividades de informação de origem eletromagnética dos EUA são necessárias e proporcionais à consecução dos objetivos de segurança nacional fixados, a criação de um novo mecanismo de recurso com autoridade independente e vinculativa e a melhoria da atual supervisão rigorosa e estratificada das atividades de informação de origem eletromagnética dos EUA. Através destas proteções, os cidadãos da UE podem obter reparação de um novo mecanismo de recurso a vários níveis, que inclui um DPRC independente, constituído por pessoas escolhidas fora do Governo dos EUA, com plena autoridade para decidir das queixas e tomar as medidas corretivas necessárias. O *Department* manterá um registo dos cidadãos da UE que apresentem uma queixa admissível nos termos do *Executive Order 14086* e do título 28, parte 201, do CFR. Cinco anos após a data da presente carta e, posteriormente, de cinco em cinco anos, o *Department* contactará os serviços competentes para saber se as informações relativas à análise das queixas admissíveis ou à análise de quaisquer pedidos de reapreciação apresentados ao DPRC foram desclassificadas. Se essas informações tiverem sido desclassificadas, o *Department* colaborará com a APD competente para informar o cidadão da UE. Estas melhorias confirmam que os dados pessoais da UE transferidos para os Estados Unidos são tratados de forma coerente com os requisitos legais da UE no que respeita ao acesso do governo aos dados.

Com base nos princípios, no *Executive Order 14086*, no título 28, parte 201, do CFR e nos ofícios e materiais que os acompanham, nomeadamente os compromissos do *Department* em relação à administração e supervisão do programa do Quadro de Privacidade de Dados, a nossa expectativa é de que a Comissão determine que o QPD 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 QPD UE-EUA. Esperamos também que as transferências para as organizações norte-americanas efetuadas com base nas cláusulas contratuais-tipo da UE ou nas regras vinculativas da UE aplicáveis às empresas sejam ainda mais facilitadas pelas condições desses acordos.

Queira aceitar a expressão da minha mais elevada consideração,



Marisa Lago

ANEXO IV

UNITED STATES OF AMERICA
Federal Trade Commission
WASHINGTON, D.C. 20580

Office of the Chair

9 de junho de 2023

Didier Reynders
Comissário da Justiça
Comissão Europeia
Rue de la Loi/Wetstraat 200
1049 Bruxelas
Bélgica

Senhor Comissário,

A Federal Trade Commission (FTC) dos Estados Unidos agradece a oportunidade de abordar o seu papel de aplicação da lei em relação aos princípios do Quadro de Privacidade de Dados UE-EUA («QPD UE-EUA»). Há muito que a FTC assumiu o compromisso de proteger os consumidores e a privacidade a nível transfronteiras, estando empenhada na aplicação dos aspetos do setor comercial deste quadro. Desde 2000, a FTC tem desempenhado esse papel em relação ao quadro do Porto Seguro EUA-UE e, mais recentemente, desde 2016, em relação ao quadro do Escudo de Proteção da Privacidade UE-EUA ([1]). Em 16 de julho de 2020, o Tribunal de Justiça da União Europeia (TJUE) declarou inválida a decisão de adequação da Comissão Europeia subjacente ao quadro do Escudo de Proteção da Privacidade UE-EUA, com base em questões diferentes dos princípios comerciais que a FTC aplicou. Desde então, os EUA e a Comissão Europeia negociaram o Quadro de Privacidade de Dados UE-EUA para dar resposta a essa decisão do TJUE.

Escrevo para confirmar o compromisso da FTC relativamente à aplicação rigorosa dos princípios do QPD UE-EUA. Designadamente, confirmamos o nosso compromisso em três domínios principais: 1) atribuição de prioridade às transmissões de queixas e investigações; 2) obtenção e acompanhamento de decisões; e 3) cooperação com as autoridades de proteção de dados (APD) da UE em matéria de execução.

I. **Introdução**

a. **Trabalhos da FTC em matéria de respeito da privacidade e elaboração de políticas neste domínio**

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 consumidores e dos seus dados. O direito primário

([1]) Carta da presidente Edith Ramirez para Věra Jourová, comissária da Justiça, Consumidores e Igualdade de Género da Comissão Europeia, que descreve a aplicação pela *Federal Trade Commission* do novo quadro do Escudo de Proteção da Privacidade UE-EUA (29 de fevereiro de 2016), *disponível em:* https://www.ftc.gov/legal-library/browse/cases-proceedings/public-statements/letter--chairwoman-edith-ramirez-vera-jourova-commissioner-justice-consumers-gender-equality-european. A FTC também se comprometeu anteriormente a aplicar o programa Porto Seguro EUA-UE. Carta de Robert Pitofsky, presidente da FTC, para John Mogg, diretor da DG Mercado Interno, Comissão Europeia (14 de julho de 2000), *disponível em:* https://www.federalregister.gov//documents/2000/07/24/00-18489/issuance-of-safe-harbor-principles-and-transmission-to-european-commission. Esta carta substitui esses compromissos assumidos anteriormente.

aplicado pela FTC, a *FTC Act* (lei relativa à Comissão reguladora do comércio federal), proíbe atos ou práticas «desleais» ou «enganosos» relativos aos comércio ([2]). 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 ([3]).

Recentemente, a FTC também levou a cabo várias iniciativas para reforçar o seu trabalho em matéria de privacidade. Em agosto de 2022, a FTC anunciou que está a considerar regras para reprimir a vigilância comercial prejudicial e a falta de segurança dos dados ([4]). O objetivo do projeto é criar um registo público sólido para informar se a FTC deve emitir regras para abordar a vigilância comercial e as práticas de segurança de dados e como devem ser essas regras. As partes interessadas da UE enviaram observações sobre esta e outras iniciativas.

As nossas conferências «PrivacyCon» continuam a reunir os principais investigadores para discutir as últimas investigações e tendências relacionadas com a privacidade dos consumidores e a segurança dos dados. Também aumentámos a capacidade da nossa agência para acompanhar a evolução tecnológica que está no centro de grande parte do nosso trabalho relativo à privacidade, criando uma equipa em expansão de tecnólogos e investigadores interdisciplinares. Como é do seu conhecimento, anunciámos ainda um diálogo conjunto com Vossa Excelência e com os seus colegas da Comissão Europeia, que inclui a abordagem de temas relacionados com a privacidade, como os padrões obscuros e os modelos de negócio caracterizados pela recolha de dados generalizada ([5]). Também emitimos recentemente um relatório ao Congresso alertando para os danos associados à utilização da inteligência artificial (IA), para resolver os danos em linha identificados pelo Congresso. Este relatório suscitou preocupações quanto à inexatidão, parcialidade, discriminação e vigilância comercial ([6]).

b. **Proteções legais dos EUA que beneficiam os consumidores da UE**

O QPD UE-EUA funcionará no contexto do panorama mais amplo da privacidade nos EUA, que protege os consumidores da UE de várias formas. 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 concreto nos Estados Unidos. Além disso, para a proteção dos consumidores estrangeiros, a FTC pode utilizar todas as reparações disponíveis para a proteção dos consumidores nacionais ([7]).

Além disso, a FTC aplica outras leis seletivas cujas proteções são alargadas aos consumidores de países terceiros, 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, disso informem os pais e obtenham o consentimento parental verificável. Os serviços e sítio Web

([2]) 15 U.S.C. § 45 (a). A FTC não tem competência em questões de aplicação do direito penal nem de segurança nacional. A FTC não pode, tampouco, apreciar 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, de facto tenham 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. Em alguns casos, a competência da FTC é concomitante com a de outros órgãos e agentes de autoridade. 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.

([3]) Ver *FTC, Privacy and Security*, https://www.ftc.gov/business-guidance/privacy-security.

([4]) Ver Comunicado de Imprensa, FTC, *FTC Explores Rules Cracking Down on Commercial Surveillance and Lax Data Security Practices* (11 de agosto de 2022), https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-explores-rules-cracking-down-commercial-surveillance-lax-data-security-practices.

([5]) Ver a declaração conjunta à imprensa de Didier Reynders, comissário da Justiça da Comissão Europeia, e Lina Khan, presidente da *Federal Trade Commission* dos Estados Unidos (30 de março de 2022, https://www.ftc.gov/system/files/ftc_gov/pdf/Joint%20FTC-EC%20Statement%20informal%20dialogue%20consumer%20protection%20issues.pdf.

([6]) Ver Comunicado de Imprensa, FTC, *FTC Report Warns About Using Artificial Intelligence to Combat Online Problems* (16 de junho de 2022), https://www.ftc.gov/news-events/news/press-releases/2022/06/ftc-report-warns-about-using-artificial-intelligence-combat-online-problems.

([7]) 15 U.S.C. § 45 (i)(4)(B). Além disso, «atos ou práticas desleais ou enganosas» incluem os atos ou as práticas que envolvem o comércio externo que: i) causam ou são suscetíveis de causar danos razoavelmente previsíveis nos Estados Unidos; ou ii) implicam a ocorrência de uma conduta significativa nos Estados Unidos. 15 U.S.C. § 45(a)(4)(A).

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. Além disso, para lá das leis federais dos EUA aplicadas pela FTC, outras leis federais e estaduais relativas à privacidade, à proteção do consumidor e à violação de dados podem proporcionar benefícios adicionais aos consumidores da UE.

c. **Atividade de aplicação da FTC**

A FTC instaurou processos nos termos tanto do quadro do Porto Seguro EUA-UE como no quadro do Escudo de Proteção da Privacidade UE-EUA e continuou a aplicar o Escudo de Proteção da Privacidade UE-EUA mesmo depois de o TJUE ter declarado inválida a decisão de adequação subjacente ao quadro do Escudo de Proteção da Privacidade UE-EUA ([8]). Várias das recentes queixas da FTC incluíram acusações de que as empresas violaram as disposições do Escudo de Proteção da Privacidade UE-EUA, nomeadamente em processos contra o Twitter ([9]), a CafePress ([10]) e a Flo ([11]). No processo contra o Twitter, a FTC obteve 150 milhões de USD do Twitter pela violação de uma decisão anterior da FTC relativa a práticas que afetam mais de 140 milhões de clientes, incluindo a violação do princípio 5 do Escudo de Proteção da Privacidade UE-EUA (integridade dos dados e limitação das finalidades). Além disso, a decisão da agência exige que o Twitter permita que os utilizadores utilizem métodos de autenticação multifatores seguros que não exijam que os utilizadores forneçam os seus números de telefone.

No processo CafePress, a FTC alegou que a empresa não protegeu as informações sensíveis dos consumidores, encobriu uma grave violação de dados e violou os princípios 2 (escolha), 4 (segurança) e 6 (acesso) do Escudo de Proteção da Privacidade UE-EUA. A decisão da FTC exige que a empresa substitua as medidas de autenticação inadequadas por autenticação multifatores, limite significativamente a quantidade de dados que recolhe e conserva, cifre os números de segurança social e que um terceiro avalie os seus programas de segurança da informação e forneça à FTC uma cópia que possa ser divulgada.

No processo Flo, a FTC alegou que a aplicação de acompanhamento da fertilidade divulgou dados de saúde dos utilizadores a fornecedores de análise de dados terceiros após o compromisso de manter esses dados privados. A queixa da FTC refere especificamente as interações da empresa com os consumidores da UE e que a Flo violou os princípios 1 (aviso), 2 (escolha), 3 (responsabilização pela transferência ulterior) e 5 (integridade dos dados e limitação das finalidades) do Escudo de Proteção da Privacidade UE-EUA. Entre outros aspetos, a decisão da agência exige que a Flo notifique os utilizadores afetados da divulgação das suas informações pessoais e que dê instruções a qualquer terceiro que tenha recebido dados de saúde dos utilizadores para destruir esses dados. Importa mencionar que os despachos da FTC protegem todos os consumidores a nível mundial que interajam com uma empresa e não apenas os consumidores que tenham apresentado queixas.

Muitos processos anteriores relacionados com a aplicação do Porto Seguro EUA-UE e do Escudo de Proteção da Privacidade UE-EUA envolveram organizações que concluíram uma autocertificação inicial através do *Department of Commerce*, mas não mantiveram a sua autocertificação anual enquanto continuaram a apresentar-se como participantes atuais. Outros processos envolviam falsas alegações de participação por parte de organizações que nunca concluíram uma autocertificação inicial através do *Department of Commerce*. No futuro, esperamos concentrar os nossos esforços proativos de aplicação nos tipos de violações significativas dos princípios do QPD UE-EUA alegadas em processos como o Twitter, CafePress e Flo. Enquanto isso, o *Department of Commerce* administrará e supervisionará o processo de autocertificação, manterá a lista oficial de participantes do QPD UE-EUA e tratará de outras questões relacionadas com reclamações de participação no programa ([12]). É importante notar que as organizações que alegam estar a participar no QPD UE-EUA podem estar sujeitas à aplicação efetiva dos princípios do QPD UE-EUA, mesmo que não efetuem ou mantenham a sua autocertificação através do *Department of Commerce*.

([8]) *Ver*, no apêndice A, a lista das questões relacionadas com o Porto Seguro e com o Escudo de Proteção da Privacidade da FTC.

([9]) Ver Comunicado de Imprensa, FTC, *FTC Charges Twitter with Deceptively Using Account Security Data to Sell Targeted Ads* (25 de maio de 2022), https://www.ftc.gov/news-events/news/press-releases/2022/05/ftc-charges-twitter-deceptively-using-account-security-data-sell-targeted-ads.

([10]) Ver Comunicado de Imprensa, FTC, *FTC Takes Action Against CafePress for Data Breach Cover Up* (15 de março de 2022), https://www.ftc.gov/news-events/news/press-releases/2022/03/ftc-takes-action-against-cafepress-data-breach-cover.

([11]) Ver Comunicado de Imprensa, FTC, *FTC Finalizes Order with Flo Health, a Fertility-Tracking App that Shared Sensitive Health Data with Facebook, Google, and Others* (22 de junho de 2021), https://www.ftc.gov/news-events/news/press-releases/2021/06/ftc-finalizes-order-flo-health-fertility-tracking-app-shared-sensitive-health-data-facebook-google.

([12]) Ofício de Marisa Lago, *Under Secretary of Commerce for International Trade*, dirigida a S. Ex.ª o Comissário da Justiça Didier Reynders, Comissão Europeia (12 de dezembro de 2022).

II. **Priorização e instrução das queixas apresentadas**

Tal como realizámos no âmbito do quadro do Porto Seguro EUA-UE e do quadro do Escudo de Proteção da Privacidade UE-EUA, a FTC compromete-se a dar prioridade à consideração de queixas relacionadas com os princípios do QPD UE-EUA apresentadas pelo *Department of Commerce* e pelos Estados-Membros da UE. Também daremos prioridade à consideração de queixas de incumprimento dos princípios do QPD UE-EUA submetidas por organizações de autorregulamentação em matéria de privacidade e por outros organismos independentes de resolução de litígios.

Para facilitar a apresentação de queixas no âmbito do QPD UE-EUA provenientes dos Estados-Membros da UE, a FTC criou um processo de transmissão de queixas normalizado e a forneceu 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 nomeu 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 dessa queixa submetida pelo *Department of Commerce*, por um Estado-Membro da UE ou por uma organização de autorregulamentação ou por outros organismos independentes de resolução de litígios, a FTC pode tomar várias medidas para resolver os problemas levantados. 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.

Para além de dar prioridade às queixas relacionadas com os princípios do QPD UE-EUA submetidas pelo Department of Commerce, pelos Estados-Membros da UE e pelas organizações de autorregulamentação em matéria de privacidade ou por outros organismos independentes de resolução de litígios ([13]), a FTC continuará a investigar violações significativas dos princípios do QPD UE-EUA por sua própria iniciativa, sempre que adequado, utilizando uma série de ferramentas. No âmbito do programa da FTC de investigação de questões relativas à privacidade e à segurança que envolvam organizações comerciais, a agência analisava regularmente se a entidade em causa fazia afirmações sobre o Escudo de Proteção da Privacidade UE-EUA. Se a entidade fizesse tais afirmações e a investigação revelasse violações aparentes dos princípios do Escudo de Proteção da Privacidade UE-EUA, a FTC incluía alegações de violações do Escudo de Proteção da Privacidade UE-EUA nas suas medidas coercivas. Continuaremos com esta abordagem proativa, atualmente no que diz respeito aos princípios do QPD UE-EUA.

III. **Obtenção e acompanhamento de decisões**

A FTC confirma ainda o seu compromisso de obter e acompanhar as decisões de execução para assegurar o cumprimento dos princípios do QPD UE-EUA. Exigiremos o cumprimento dos princípios do QPD UE-EUA através de várias disposições de injunção adequadas em futuras decisões da FTC relativas aos princípios do QPD UE-EUA. As violações dos despachos administrativos da FTC podem conduzir a sanções de caráter civil máximas de 50 120 USD por violação ou 50 120 USD por dia por uma violação contínua ([14]),que, no caso de práticas que afetam muitos consumidores, pode ascender a milhões de dólares norte-americanos. Cada injunção contém também disposições em matéria de comunicação e cumprimento. 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 acompanha sistematicamente o cumprimento das decisões existentes relativas aos princípios do Escudo de Proteção da Privacidade UE-EUA, tal como procede com todas as suas decisões, e intenta ações para as fazer cumprir, sempre que necessário ([15]). Importa mencionar que os despachos da FTC continuarão a proteger todos os consumidores a nível mundial que interajam com uma empresa e não apenas os consumidores que tenham apresentado queixas. Por último, a FTC manterá uma lista em linha das empresas objeto de decisões obtidas no âmbito da aplicação dos princípios do QPD UE-EUA ([16]).

([13]) Embora a FTC não proceda à resolução ou mediação de queixas de consumidores a título individual, a FTC confirma que atribuirá prioridade às queixas no âmbito dos princípios do QPD UE-EUA 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 acessível aos consumidores norte-americanos para apresentar uma queixa à FTC, disponível em https://reportfraud.ftc.gov/. Contudo, no que se refere às queixas individuais relativas ao QPD UE-EUA, pode ser mais útil para os cidadãos da UE apresentar queixas à APD ou ao organismo independente de resolução de litígios do seu Estado-Membro.

([14]) 15 U.S.C. § 45(m); 16 C.F.R. § 1.98. Este montante é periodicamente ajustado em função da inflação.

([15]) No ano passado, a FTC votou no sentido de simplificar o processo de investigação de infratores reincidentes. Ver Comunicado de Imprensa, FTC, *FTC Authorizes Investigations into Key Enforcement Priorities* (1 de julho de 2021), https://www.ftc.gov/news-events/news/press-releases/2021/07/ftc-authorizes-investigations-key-enforcement-priorities.

([16]) *Cf.* FTC, *Privacy Shield*, https://www.ftc.gov/business-guidance/privacy-security/privacy-shield.

IV. **Cooperação em matéria de execução com as APD da UE**

A FTC reconhece o papel importante que as APD desempenham no que se refere ao cumprimento dos princípios do QPD UE-EUA e incentiva o aumento das consultas e da cooperação em matéria de execução. Com efeito, é cada vez mais crítica uma abordagem coordenada para os desafios colocados pela atual evolução do mercado digital e pelos modelos de negócio com utilização intensiva de dados. A FTC procederá ao intercâmbio de informações sobre as queixas com as autoridades responsáveis pelas medidas coercivas que apresentaram essas 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 devem incluir 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, cabe à FTC transmitir informações de retorno à 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 responde, tomando em consideração o número de queixas em análise e em conformidade com os requisitos de confidencialidade e outros requisitos jurídicos.

A FTC deve ainda trabalhar 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 ([17]). 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, em conformidade com os 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.

Para além de quaisquer consultas com as APD da UE que apresentem queixas sobre questões específicas de determinado processo, a FTC participará em reuniões periódicas com os representantes designados do Comité Europeu para a Proteção de Dados (CEPD) para debater, em termos gerais, como melhorar a cooperação em matéria de execução. 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. A FTC tem o prazer de confirmar o seu compromisso em aplicar os aspetos do setor comercial do QPD UE-EUA. Consideramos que a nossa parceria com os colegas da UE é uma parte essencial da proteção da privacidade para ambos os nossos cidadãos.

Queira aceitar a expressão da minha mais elevada consideração,

Lina M. Khan
Presidente, Federal Trade Commission

([17]) 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 vai prestar 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.

Apêndice A

Aplicação do Escudo de Proteção da Privacidade e do Porto Seguro

	Registo/número de processo da FTC	Processo	Ligação
1.	Número do processo da FTC: 2023062 Número do processo 3:22-cv-03070 (N. D. Cal.)	Estados Unidos/**Twitter, Inc.**	Twitter
2.	Número do processo da FTC: 192 3209	Processo Residual Pumpkin Entity, LLC, anteriormente com a denominação comercial **CafePress** e PlanetArt, LLC, denominação comercial **CafePress**	CafePress
3.	Número do processo da FTC: 192 3133 Número de registo C-4747	Processo **Flo Health, Inc.**	Flo Health
4.	Número do processo da FTC: 192 3050 Número de registo C-4723	Processo **Ortho-Clinical Diagnostics, Inc.**	Ortho-Clinical
5.	Número do processo da FTC: 192 3092 Número de registo C-4709	Processo **T&M Protection, LLC**	T&M Protection
6.	Número do processo da FTC: 192 3084 Número de registo C-4704	Processo **TDARX, Inc.**	TDARX
7.	Número do processo da FTC: 192 3093 Número de registo C-4706	Processo **Global Data Vault, LLC**	Global Data
8.	Número do processo da FTC: 192 3078 Número de registo C-4703	Processo **Incentive Services, Inc.**	Incentive Services
9.	Número do processo da FTC: 192 3090 Número de registo C-4705	Processo **Click Labs, Inc.**	Click Labs
10.	Número do processo da FTC: 182 3192 Número de registo C-4697	Processo **Medable, Inc.**	Medable
11.	Número do processo da FTC: 182 3189 Número de registo 9386	Processo NTT Global Data Centers Americas, Inc., como sub-rogatário dos seus interesses **RagingWire Data Centers, Inc.**	RagingWire
12.	Número do processo da FTC: 182 3196 Número de registo C-4702	Processo **Thru, Inc.**	Thru
13.	Número do processo da FTC: 182 3188 Número de registo C-4698	Processo **DCR Workforce, Inc.**	DCR Workforce
14.	Número do processo da FTC: 182 3194 Número de registo C-4700	Processo **LotaData, Inc.**	LotaData
15.	Número do processo da FTC: 182 3195 Número de registo C-4701	Processo **EmpiriStat, Inc.**	EmpiriStat

16.	Número do processo da FTC: 182 3193 Número de registo C-4699	Processo 214 Technologies, Inc., também com a denominação comercial **Trueface.ai**	Trueface.ai
17.	Número do processo da FTC: 182 3107 Número de registo 9383	Processo **Cambridge Analytica, LLC**	Cambridge Analytica
18.	Número do processo da FTC: 182 3152 Número de registo C-4685	Processo **SecureTest, Inc.**	SecurTest
19.	Número do processo da FTC: 182 3144 Número de registo C-4664	Processo **VenPath, Inc.**	VenPath
20.	Número do processo da FTC: 182 3154 Número de registo C-4666	Processo **SmartStart Employment Screening, Inc.**	SmartStart
21.	Número do processo da FTC: 182 3143 Número de registo C-4663	Processo **mResourceLLC**, denominação comercial Loop Works LLC	mResource
22.	Número do processo da FTC: 182 3150 Número de registo C-4665	Processo **Idmission LLC**	IDmission
23.	Número do processo da FTC: 182 3100 Número de registo C-4659	Processo **ReadyTech Corporation**	ReadyTech
24.	Número do processo da FTC: 172 3173 Número de registo C-4630	Processo **Decusoft, LLC**	Decusoft
25.	Número do processo da FTC: 172 3171 Número de registo C-4628	Processo **Tru Communication, Inc.**	Tru
26.	Número do processo da FTC: 172 3172 Número de registo C-4629	Processo **Md7, LLC**	Md7
30.	Número do processo da FTC: 152 3198 Número de registo C-4543	Processo **Jhayrmaine Daniels (denominação comercial California Skate-Line)**	Jhayrmaine Daniels
31.	Número do processo da FTC: 152 3190 Número de registo C-4545	Processo **Dale Jarrett Racing Adventure, Inc.**	Dale Jarrett
32.	Número do processo da FTC: 152 3141 Número de registo C-4540	Processo **Golf Connect, LLC**	Golf Connect
33.	Número do processo da FTC: 152 3202 Número de registo C-4546	Processo **Inbox Group, LLC**	Inbox Group
34.	Número do processo da FTC: 152 3187 Número de registo C-4542	Processo **IOActive, Inc.**	IOActive
35.	Número do processo da FTC: 152 3140 Número de registo C-4549	Processo **Jubilant Clinsys, Inc.**	Jubilant
36.	Número do processo da FTC: 152 3199 Número de registo C-4547	Processo **Just Bagels Manufacturing, Inc.**	Just Bagels

37.	Número do processo da FTC: 152 3138 Número de registo C-4548	Processo **NAICS Association, LLC**	NAICS
38.	Número do processo da FTC: 152 3201 Número de registo C-4544	Processo **One Industries Corp.**	One Industries
39.	Número do processo da FTC: 152 3137 Número de registo C-4550	Processo **Pinger, Inc.**	Pinger
40.	Número do processo da FTC: 152 3193 Número de registo C-4552	Processo **SteriMed Medical Waste Solutions**	SteriMed
41.	Número do processo da FTC: 152 3184 Número de registo C-4541	Processo **Contract Logix, LLC**	Contract Logix
42.	Número do processo da FTC: 152 3185 Número de registo C-4551	Processo **Forensics Consulting Solutions, LLC**	Forensics Consulting
43.	Número do processo da FTC: 152 3051 Número de registo C-4526	Processo **American Int'l Mailing, Inc.**	AIM
44.	Número do processo da FTC: 152 3015 Número de registo C-4525	Processo **TES Franchising, LLC**	TES
45.	Número do processo da FTC: 142 3036 Número de registo C-4459	Processo **American Apparel, Inc.**	American Apparel
46.	Número do processo da FTC: 142 3026 Número de registo C-4469	Processo **Fantage.com, Inc.**	Fantage
47.	Número do processo da FTC: 142 3017 Número de registo C-4461	Processo **Apperian, Inc.**	Apperian
48.	Número do processo da FTC: 142 3018 Número de registo C-4462	Processo **Atlanta Falcons Football Club, LLC**	Atlanta Falcons
49.	Número do processo da FTC: 142 3019 Número de registo C-4463	Processo **Baker Tilly Virchow Krause, LLP**	Baker Tilly
50.	Número do processo da FTC: 142 3020 Número de registo C-4464	Processo **BitTorrent, Inc.**	BitTorrent
51.	Número do processo da FTC: 142 3022 Número de registo C-4465	Processo **Charles River Laboratories, Int'l**	Charles River
52.	Número do processo da FTC: 142 3023 Número de registo C-4466	Processo **DataMotion, Inc.**	DataMotion
53.	Número do processo da FTC: 142 3024 Número de registo C-4467	Processo **DDC Laboratories, Inc.**, denominação comercial DNA Diagnostics Center	DDC
54.	Número do processo da FTC: 142 3028 Número de registo C-4470	Processo **Level 3 Communications, LLC**	Level 3

55.	Número do processo da FTC: 142 3025 Número de registo C-4468	Processo **PDB Sports, Ltd.**, denominação comercial the Denver Broncos Football Club, LLP	Broncos
56.	Número do processo da FTC: 142 3030 Número de registo C-4471	Processo **Reynolds Consumer Products, Inc.**	Reynolds
57.	Número do processo da FTC: 142 3031 Número de registo C-4472	Processo **Receivable Management Services Corporation**	Receivable Mgmt
58.	Número do processo da FTC: 142 3032 Número de registo C-4473	Processo **Tennessee Football, Inc.**	Tennessee Football
59.	Número do processo da FTC: 102 3058 Número de registo C-4369	Processo **Myspace LLC**	Myspace
60.	Número do processo da FTC: 092 3184 Número de registo C-4365	Processo **Facebook, Inc.**	Facebook
61.	Número do processo da FTC: 092 3081 Ação civil n.º 09-CV-5276 (C. D. Cal.)	FTC/Javian Karnani e **Balls of Kryptonite, LLC**, denominação comercial Size Deals, LLC e Best Priced Brands, LLC	Balls of Kryptonite
62.	Número do processo da FTC: 102 3136 Número de registo C-4336	Processo **Google, Inc.**	Google
63.	Número do processo da FTC: 092 3137 Número de registo C-4282	Processo **World Innovators, Inc.**	World Innovators
64.	Número do processo da FTC: 092 3141 Número de registo C-4271	Processo **Progressive Gaitways LLC**	Progressive Gaitways
65.	Número do processo da FTC: 092 3139 Número de registo C-4270	Processo **Onyx Graphics, Inc.**	Onyx Graphics
66.	Número do processo da FTC: 092 3138 Número de registo C-4269	Processo **ExpatEdge Partners, LLC**	ExpatEdge
67.	Número do processo da FTC: 092 3140 Número de registo C-4281	Processo **Directors Desk LLC**	Directors Desk
68.	Número do processo da FTC: 092 3142 Número de registo C-4272	Processo **Collectify LLC**	Collectify

ANEXO V

THE SECRETARY OF TRANSPORTATION
WASHINGTON, DC 20590

6 de julho de 2023

Comissário Didier Reynders
Comissão Europeia
Rue de la Loi/Wetstraat 200
1049 1049 Bruxelas
Bélgica

Senhor Comissário,

O *Department of Transportation* (*Department* ou «DOT») dos Estados Unidos aprecia a oportunidade de descrever o seu papel na aplicação dos princípios do Quadro de Privacidade de Dados («QPD UE-EUA») UE-EUA. O QPD UE-EUA desempenhará um papel fundamental na proteção dos dados pessoais fornecidos durante transações comerciais 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.

Numa carta enviada à Comissão Europeia há mais de 22 anos, o DOT manifestou publicamente, pela primeira vez, o seu compromisso de aplicar o quadro do Porto Seguro EUA-UE, compromisso que foi renovado e alargado numa carta de 2016 relativa ao quadro do Escudo de Proteção da Privacidade UE-EUA. Nessas cartas, o DOT comprometeu-se a aplicar os princípios da privacidade do Porto Seguro EUA-UE de modo rigoroso e, posteriormente, os princípios do Escudo de Proteção da Privacidade UE-EUA. O DOT alarga este compromisso aos princípios do QPD UE-EUA, recordando, a presente carta, esse compromisso.

Nomeadamente, o DOT confirma o seu compromisso nos seguintes domínios fundamentais: 1) atribuição de prioridade à investigação de alegadas violações dos princípios do QPD UE-EUA; 2) adoção de medidas coercivas adequadas contra as entidades que façam alegações falsas ou enganosas de participação no QPD UE-EUA; e 3) acompanhamento e publicação de decisões de execução relativas a violações dos princípios do QPD UE-EUA. 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 dos princípios do QPD UE-EUA.

1. **Antecedentes**

A. Autoridade do DOT em matéria de proteção da privacidade

O *Department* está 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 responsável por adotar medidas neste domínio está estabelecida em 49 U.S.C. 41712, que proíbe uma transportadora ou uma agência de viagens de adotar «práticas desleais ou enganosas» no transporte aéreo ou na venda de passagens aéreas. A secção 41712 segue o modelo da secção 5 da *Federal Trade Commission Act* (FTC) (15 U.S.C. 45).

Recentemente, o DOT emitiu regulamentos que definem as práticas desleais ou enganosas, coerentes com os precedentes do DOT e da FTC (14 CFR § 399.79). Em específico, uma prática é «desleal» se causar, ou for suscetível de causar, danos substanciais, que não sejam razoavelmente evitáveis, e se os danos não forem compensados por benefícios para os consumidores ou para a concorrência.

Uma prática é «enganosa» para os consumidores se for suscetível de induzir em erro um consumidor, agindo razoavelmente de acordo com as circunstâncias, no que respeita a uma questão prejudicial. Uma questão é prejudicial se for suscetível de afetar o comportamento ou a decisão do consumidor em relação a um produto ou serviço. Para além destes princípios gerais, o DOT interpreta especificamente a secção 41712 no sentido de proibir as transportadoras e as agências de viagens de: 1) violar as disposições previstas na sua política de privacidade; 2) violar qualquer regra emitida pelo *Department of Transportation* que identifique práticas específicas relativas à privacidade como desleais ou enganosas; ou 3) violar a *Children's Online Privacy Protection Act* (COPPA) ou a regras da FTC que aplicam a COPPA. ou 4) não cumprir, na qualidade de aderente ao QPD UE-EUA, os princípios do QPD UE-EUA ([1]).

Tal como anteriormente referido, 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 do QPD UE-EUA, 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 do QPD UE-EUA, 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 Consumer Protection* (OACP) ([2]) do *Department* realiza investigações e intenta ações nos termos do 49 U.S. C. 41712. 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 ([3]).

Caso não se chegue a um acordo razoável e adequado num determinado caso, o OACP 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 37 377 USD por cada violação da secção 41712.

O *Department of Transportation* não tem competência para conceder indemnizações nem reparações pecuniárias aos queixosos a título individual. 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 e 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 QPD UE-EUA se as circunstâncias o justificarem. Uma violação repetida da secção 41 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, essas queixas são investigadas em conformidade com os princípios estabelecidos acima.

C. Proteções legais 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 as práticas da companhia aérea terem ocorrido no âmbito da prestação de transporte de ou para os Estados Unidos. O DOT utiliza e vai continuar 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.

([1]) https://www.transportation.gov/individuals/aviation-consumer-protection/privacy.
([2]) Anteriormente conhecido por *Office of Aviation Enforcement and Proceedings*.
([3]) http://www.transportation.gov/airconsumer/privacy-complaints.

Além disso, a DOT aplica , no que diz respeito às companhias aéreas, outras leis seletivas cujas proteções são alargadas aos consumidores de países terceiros, 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 reconhecidamente recolhem informações pessoais de crianças com idade inferior a 13 anos, informem disso os pais e obtenham o consentimento parental verificável. 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 EUA violarem a COPPA, o DOT teria competência para tomar medidas coercitivas.

II. **Aplicação dos princípios do QPD UE-EUA**

Se uma companhia aérea ou uma agência de viagens optar por participar no quadro do QPD UE-EUA e o *Department of Transportation* receber uma queixa de que tal companhia aérea ou agência de viagens alegadamente violou os princípios do QPD UE-EUA, o *Department of Transportation* tomaria as medidas abaixo para aplicar decididamente os princípios do QPD UE-EUA.

A. Atribuição de prioridade à investigação de alegadas violações

O OACP do *Department* investigará todas as queixas que aleguem violações dos princípios do QPD UE-EUA, nomeadamente as queixas apresentadas pelas autoridades de proteção de dados (APD) da UE, e adotará medidas coercivas sempre que existam provas de uma violação.

Além disso, o OACP cooperará com a FTC e com o *Department of Commerce* e atribuirá prioridade às alegações de que as entidades reguladas não respeitam os compromissos em matéria de privacidade assumidos no âmbito do QPD UE-EUA.

Após a submissão de uma alegação de violação dos princípios do QPD UE-EUA, o OACP pode adotar uma série de 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 questões da competência do *Department of Commerce* ou da FTC, avaliaria o benefício da sensibilização dos consumidores e das empresas e, conforme adequado, daria início a um processo de execução.

Caso o *Department* tome conhecimento de possíveis violações dos princípios do QPD UE-EUA 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 aos princípios do QPD UE-EUA.

B. Resolução de alegações falsas ou enganosas de participação

O *Department* continua empenhado em investigar as violações dos princípios do QPD UE-EUA, nomeadamente as alegações falsas ou enganosas de participação no QPD UE-EUA. Atribuiremos prioridade à apreciação das queixas submetidas pelo *Department of Commerce* sobre organizações que identifique que aleguem indevidamente ser aderentes atuais do QPD UE-EUA ou que utilizem a respetiva marca de certificação sem autorização.

Além disso, salientamos que se a política de privacidade de uma empresa promete que cumpre os princípios do QPD UE-EUA, a não efetuação ou manutenção de autocertificação através do *Department of Commerce* provavelmente não irá, por si só, isentar a organização da execução desses compromissos por parte do DOT.

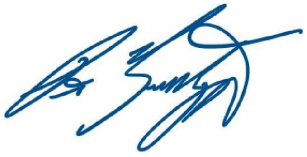
C. Acompanhamento e publicação de decisões de execução relativas às violações do QPD UE-EUA

O OACP do *Department* também continua empenhado no acompanhamento das decisões de execução, conforme necessário, para assegurar a conformidade com os princípios do QPD UE-EUA. Especificamente, se a referida entidade emitir uma decisão que cesse ou proíba futuras violações, por parte de uma companhia aérea ou agência de viagens, dos princípios do QPD UE-EUA e da secção 41712, compete a essa entidade controlar o cumprimento da disposição de cessação ou proibição constante da decisão. Além disso, a referida entidade deve assegurar que as decisões resultantes dos processos relativos aos princípios do QPD UE-EUA estão 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 QPD UE-EUA.

Espero que estas informações sejam úteis e estou ao inteiro dispor de Vossa Excelência para quaisquer dúvidas ou outras informações de que necessite.

Queira aceitar a expressão da minha mais elevada consideração,



Pete Buttigieg

ANEXO VI

U.S. Department of Justice

Criminal Division

Office of Assistant Attorney General Washington, D.C. 20530

23 de junho de 2023

Ana Gallego Torres
Direção-Geral da Justiça e dos Consumidores
Comissão Europeia
Rue Montoyer/Montoyerstraat 59
1049 Bruxelas
Bélgica

Excelentíssima Senhora diretora-geral Gallego Torres:

O presente ofício 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]). Todos os processos legais descritos no presente ofício não são discriminatórios, desde que utilizados para obter informações de empresas nos Estados Unidos, nomeadamente de empresas que se autocertificaram através do Quadro de Privacidade de Dados UE-EUA, sem tomar em consideração a nacionalidade ou o local de residência do titular dos dados. Além disso, as empresas que são objeto de um tratamento legal dos seus dados nos Estados Unidos podem impugná-lo judicialmente, conforme descrito infra ([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 pode ser infringido, e nenhum mandado é 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 impõe que os agentes responsáveis pela da lei tenham um mandado emitido pelo tribunal antes da realização de uma busca. Ver Katz v. United States, 389 U.S. 347, 357 (1967). As normas relativas à emissão de um mandado, como os requisitos de causa provável e de particularidade, são aplicáveis aos mandados de busca e apreensão físicas, bem como aos mandados relativos ao conteúdo armazenado de

([1]) A presente panorâmica não descreve os instrumentos de investigação da segurança nacional utilizados pelos órgãos de autoridade 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, 12 U.S.C. § 3414; 15 U.S.C. § 1681u; 15 U.S.C. § 1681v; 18 U.S.C. § 2709, 50 U.S.C. § 3162, e, no que diz respeito à vigilância eletrónica, mandados de busca, documentação empresarial e outra recolha de informações nos termos da *Foreign Intelligence Surveillance Act*, 50 U.S.C. § 1801 et seq.

([2]) O presente ofício aborda as competências regulamentares e de aplicação da legislação federal. As violações do legislação estadual são investigadas pelas autoridades estaduais e são apreciadas em tribunais estaduais. As autoridades estaduais responsáveis pela aplicação da lei utilizam mandatos e intimações emitidos nos termos do direito estadual essencialmente da forma descrita no presente documento, mas com a possibilidade de o processo judicial estadual ser objeto de proteções previstas pelas constituições ou pelas leis estaduais que ultrapassam as da Constituição dos EUA. As proteções garantidas pela legislação estadual devem ser pelo menos equivalentes às da Constituição dos EUA, incluindo, entre outras, a Quarta Emenda.

comunicações eletrónicas emitidos nos termos da *Stored Communications Act*, tal como se descreve adiante. Sempre que o requisito de mandado não seja aplicável, a atividade do governo continua a estar sujeita a um teste de «razoabilidade» nos termos da Quarta Emenda. Portanto, a própria Constituição garante que o governo dos EUA não dispõe de competências ilimitadas ou arbitrárias para apreender informações privadas ([3]).

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 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 no âmbito 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 de aplicação da lei orientadas. Uma intimação de um júri consiste num pedido oficial emitido por um júri (regra geral, 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 pertinentes para a investigação e a intimação deve permanecer razoável, ou seja, n\ao pode ser demasiado abrangente, opressiva ou onerosa. Um destinatário pode apresentar uma moção para contestar a intimação com base nesses motivos. See 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, os órgãos de autoridade 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 pertinentes 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 regem o acesso do governo às informações sobre assinantes, aos dados de tráfego e ao conteúdo armazenado de comunicações na posse de fornecedores de serviços de Internet (também conhecidos por «ISP»), empresas telefónicas 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 garantidos legalmente em matéria de privacidade que limitam o acesso dos órgãos de autoridade aos dados para além do que é necessário nos termos do direito constitucional dos clientes e assinantes de ISP. 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

([3]) No que diz respeito aos princípios da Quarta Emenda relativos à proteção da privacidade e dos interesses de segurança referidos acima, os tribunais dos EUA aplicam regularmente esses princípios aos novos tipos de instrumentos de investigação das autoridades responsáveis pela aplicação da lei viabilizados pela evolução tecnológica. Por exemplo, em 2018, o Supremo Tribunal decidiu que a obtenção pelo governo, no âmbito de uma investigação policial, de informações históricas de localização das células telefónicas de uma empresa de telemóveis durante um período alargado é uma «busca» que necessita de um mandado nos termos da Quarta Emenda. Carpenter v. Estados Unidos, 138 S. Ct. 2206 (2018)

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 pertinentes 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 ([4]).

Decisões judiciais relativas a vigilância nos termos da Federal Wiretap Law: Além disso, os órgãos de autoridade 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. §§ 2510-2523. 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.

Search Warrant-Fed. R. Crim. P. Rule 41: Os órgãos de autoridade podem realizar buscas físicas nos Estados Unidos sempre que um juiz o autorize. Os órgãos de autoridade devem demonstrar ao juiz, com base na apresentação de uma «causa provável», que um crime foi cometido ou está prestes a ser cometido e que os elementos relacionados com o crime serão provavelmente encontrados no local especificado pelo mandado. Esta competência é muitas vezes utilizada nos casos em que é necessária uma busca física a instalações pela polícia seja necessária devido ao perigo de destruição de provas se uma intimação ou outra decisão de apresentação de documentos for notificada à empresa. Um cidadão sujeito a uma busca ou cujos bens sejam objeto de busca pode apresentar um pedido de supressão das provas obtidas ou derivadas de uma busca ilegal, caso essas provas sejam apresentadas contra esse cidadão durante um processo penal. Ver *Mapp v. Ohio, 367 U.S. 643* (1961). Quando um detentor dos dados for obrigado a divulgar dados no âmbito de um mandado, a parte obrigada pode contestar o requisito de divulgação por ser excessivamente oneroso. Ver *In re Application of United States*, 610 F.2d 1148, 1157 (3d Cir.1979) (que determina que «o processo justo exige uma audiência sobre a questão da onerosidade antes de obrigar uma empresa telefónica a prestar» assistência com um mandado de busca); *In re Application of United States*, 616 F.2d 1122 (9th Cir.1980) (que chega à mesma conclusão com base na autoridade de supervisão do tribunal).

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 determinam limites adicionais ao acesso dos órgãos de autoridade aos dados e que contêm igualmente proteções relativas à privacidade e às liberdades cívicas. Por exemplo, as diretrizes do *Attorney-General* para as operações nacionais do FBI (*Attorney General's Guidelines for Domestic FBI Operations*) (setembro de 2008) (em seguida designadas «*Guidelines AG FBI*»), disponíveis emhttp://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 impõe ao FBI a utilização dos métodos de investigação menos intrusivos possíveis, tendo em conta o efeito na privacidade e nas liberdades civis de eventuais danos reputacionais. Além disso, salientam que obviamente o FBI deve realizar 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 seu guia para as operações e investigações nacionais (DIOG), disponível em https://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29, 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 estão estabelecidas no *Justice Manual*, também disponível em linha em https://www.justice.gov/jm/justicemanual.

Competências civis e regulamentares (interesse público):

([4]) Além disso, a secção 2705(b) da SCA autoriza o governo a obter uma decisão judicial com base na necessidade demonstrada de proteção contra a divulgação, que proíba um prestador de serviços de comunicações de notificar, a título voluntário, os seus utilizadores da instauração de um processo judicial nos termos da SCA. Em outubro de 2017, o *Deputy Attorney General* Rod Rosenstein emitiu um memorando destinado aos advogados e agentes do DOJ, definindo orientações para assegurar que os pedidos de tais decisões cautelares são adaptados aos factos e às preocupações específicos de uma investigação e fixando, relativamente ao pedido, um limite máximo geral de um ano para o prolongamento da notificação. Em maio de 2022, a *Deputy Attorney General* Lisa Monaco emitiu orientações suplementares sobre o tema, que, entre outras questões, estabeleciam requisitos de aprovação interna do DOJ para os pedidos de prorrogação de uma decisão cautelar para além do período inicial de um ano e exigiam a cessação das decisões cautelares no fim de uma investigação.

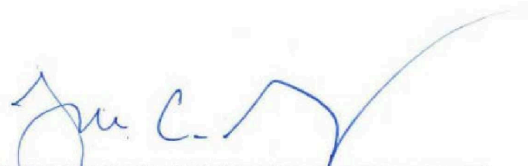
Também existem limites significativos ao acesso regulamentar ou civil (isto é, «interesse público») aos dados detidos por empresas nos Estados Unidos. Os organismos com responsabilidades civis e regulamentares podem emitir intimações a empresas para a obtenção de documentação empresarial, informações 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 jurisdicional independente das intimações antes da potencial execução judicial. Ver, por exemplo, Fed. p. 45. Os organismos podem solicitar o acesso apenas aos dados pertinentes 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, conforme exposto antes.

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. 31 U.S.C. § 5318; 31 C.F.R. capítulo X. Outras empresas podem basear-se na *Fair Credit Reporting Act*, 15 U.S.C. § 1681b, ou num conjunto de outras leis setoriais específicas. 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. §§ 3401–3423. 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 v. City of Seattle, 387 U.S. 541 (1967).

Conclusão

Todas as atividades regulamentares e de aplicação da lei nos Estados Unidos devem ser conformes com a legislação aplicável, nomeadamente a Constituição, as leis, as normas e os regulamentos dos EUA. Estas atividades também devem respeitar as políticas pertinentes, nomeadamente as diretrizes do Procurador-Geral que regem 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.



Bruce C. Swartz
Deputy Assistant Attorney General and
Counselor for International Affairs

ANEXO VII

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE OFFICE OF GENERAL COUNSEL

WASHINGTON, DC 20511

9 de dezembro de 2022

Procurador-Geral
Leslie B. Kiernan
US Department of
Commerce 1401 Constitution
Ave., NW Washington, DC 20230

Excelentíssima Senhora Kiernan,

Em 7 de outubro de 2022, o Presidente Biden assinou o *Executive Order 14086* intitulado «Enhancing Safeguards for United States Signals Intelligence Activities», que reforça o rigoroso conjunto de garantias de privacidade e liberdades cívicas aplicáveis às atividades de informação de origem eletromagnética dos EUA. Entre estas garantias contam-se a exigência de as atividades de informação de origem eletromagnética cumprirem objetivos legítimos fixados, a proibição explicita dessas atividades para efeitos de objetivos específicos proibidos, a criação de novos procedimentos para assegurar que as atividades de informação de origem eletromagnética promovem esses objetivos legítimos e não promovem objetivos proibidos, a exigência de as atividades de informação de origem eletromagnética serem realizadas apenas após uma decisão baseada numa avaliação razoável de todos os fatores pertinentes, de que as atividades são necessárias para promover uma prioridade em matéria de informações validada e unicamente na medida e de uma forma que seja proporcional à prioridade em matéria de informações validada para as quais foram autorizadas e a orientação dos elementos do setor das informações para atualizarem as suas políticas e procedimentos de modo a refletirem as garantias exigidas pelo decreto executivo relativo às garantias em matéria de informação de origem eletromagnética. Mais significativamente, o decreto executivo também introduz um mecanismo independente e vinculativo que permite aos cidadãos de «Estados elegíveis», tal como designados nos termos do decreto executivo, procurar obter reparação se considerarem que foram visados por atividades de informação de origem eletromagnética dos EUA ilegais, incluindo atividades que violem as proteções constantes do decreto executivo.

A emissão, pelo Presidente Biden, do *Executive Order 14086* marcou o culminar de mais de um ano de negociações exaustivas entre os representantes da Comissão Europeia e dos Estados Unidos e orienta as medidas que os Estados Unidos adotarão para aplicar os seus compromissos no âmbito do Quadro de Privacidade de Dados UE-EUA. Em consonância com o espírito de cooperação que deu origem ao quadro, penso ter compreendido que recebeu dois conjuntos de perguntas da Comissão Europeia sobre a forma como o setor das informações aplicará o decreto executivo. Tenho todo o gosto em responder a estas perguntas através da presente carta.

Secção 702 da Foreign Intelligence Surveillance Act de 1978 (secção 702 da FISA)

O primeiro conjunto de perguntas diz respeito à secção 702 da FISA, que permite que se visem cidadãos de países terceiros que se acredita estarem localizados fora dos Estados Unidos, com a assistência obrigatória dos prestadores norte-americanos de serviços de comunicações eletrónicas, para recolher informações externas. Especificamente, as perguntas dizem respeito à interação entre essa disposição e o *Executive Order 14086*, bem como às outras garantias aplicáveis às atividades realizadas nos termos da secção 702 da FISA.

Para começar, podemos confirmar que o setor das informações aplicará as garantias estabelecidas no *Executive Order 14086* às atividades realizadas nos termos da secção 702 da FISA.

Além disso, são aplicáveis várias outras garantias à utilização da secção 702 da FISA por parte do governo. Por exemplo, todas as certificações previstas na secção 702 da FISA devem ser assinadas tanto pelo *Attorney General* como pelo *Director of National Intelligence*, tendo o governo de submeter todas essas certificações à aprovação do *Foreign Intelligence Surveillance Court* (FISC), que é constituído por juízes independentes e com posto vitalício durante mandatos não renováveis de sete anos. As certificações identificam as categorias de informações externas a recolher, que devem satisfazer a definição legal de informações externas ao visar cidadãos de países terceiros que se acredita estarem localizados fora dos Estados Unidos. As certificações incluíram informações relativas ao terrorismo internacional e outros temas, como a obtenção de informações sobre armas de destruição maciça. Cada certificação anual deve ser submetida ao FISC para aprovação num pacote de declaração de certificação que inclui as certificações do *Attorney General* e do *Director of National Intelligence*, declarações ajuramentadas de determinados diretores dos serviços de informações e procedimentos de orientação, procedimentos de minimização e procedimentos de consulta de informação que sejam vinculativos para o governo. Os procedimentos de seleção de alvos requerem, entre outros aspetos, que o setor das informações avalie razoavelmente, com base em todas as circunstâncias, que o alvo é suscetível de conduzir à recolha de informações externas constantes de uma certificação prevista na secção 702 da FISA.

Além disso, aquando da recolha de informações nos termos da secção 702 da FISA, o setor das informações deve fornecer uma explicação por escrito dos fundamentos da sua avaliação, no momento da seleção do alvo, de que se espera que o alvo possua, receba ou provavelmente comunique informações externas constantes de uma certificação prevista na secção 702 da FISA, deve confirmar que a norma de seleção de alvos, tal como estabelecida nos procedimentos de seleção de alvos previstos na secção 702 da FISA, continua a ser cumprida e cessar a recolha se a norma deixar de ser cumprida. *Ver* a petição do Governo dos EUA ao *Foreign Intelligence Surveillance Court*, *2015 Summary of Notable Section 702 Requirements*, p. 2 a 3 (15 de julho de 2015).

Exigir que o setor das informações registe por escrito e confirme regularmente a validade da sua avaliação de que os alvos selecionados nos termos da secção 702 da FISA cumprem as normas de definição de alvos aplicáveis facilita a supervisão pelo FISC das atividades de seleção de alvos do setor das informações. Cada avaliação e fundamentação registada dos alvos é analisada de dois em dois meses pelos advogados de supervisão dos serviços de informações no *Department of Justice* (DOJ), que desempenham esta função de supervisão à parte das operações de recolha de informações externas. A secção do DOJ que desempenha esta função é responsável, nos termos de uma regra do FISC há muito estabelecida, por comunicar ao FISC quaisquer violações dos procedimentos aplicáveis. Esta comunicação, juntamente com as reuniões regulares entre o FISC e esta secção do DOJ responsável pela supervisão da seleção de alvos nos termos da secção 702 da FISA, permite ao FISC garantir o cumprimento da seleção de alvos ao abrigo da secção 702 da FISA e de outros procedimentos e, de outro modo, assegurar a legalidade das atividades do governo. Em especial, o FISC pode fazê-lo de várias formas, nomeadamente através da emissão de decisões de medidas corretivas vinculativas dirigidas à autoridade do governo para interromper a recolha de dados contra um determinado alvo ou para alterar ou adiar a recolha de dados nos termos da secção 702 da FISA. O FISC também pode exigir que o governo forneça mais relatórios ou informações sobre o seu cumprimento relativamente à seleção de alvos e outros procedimentos ou exigir alterações desses procedimentos.

Recolha «em larga escala» de informação de origem eletromagnética

O segundo conjunto de perguntas diz respeito à recolha «em larga escala» de informação de origem eletromagnética, que é definida pelo *Executive Order 14086* como «a recolha autorizada de grandes quantidades de dados de origem eletromagnética que, por motivos técnicos ou operacionais, são obtidos sem recurso a discriminantes (por exemplo, sem recurso a identificadores ou termos de seleção específicos)».

No que respeita a estas perguntas, note-se, em primeiro lugar, que nem a FISA nem as *National Security Letters* autorizam a recolha em larga escala. Relativamente à FISA:

— Os Títulos I e III da FISA, que, respetivamente, autorizam a vigilância eletrónica e buscas físicas, implicam uma decisão judicial (com exceções limitadas, como em casos urgentes) e requerem sempre uma causa provável para considerar que o alvo é uma potência estrangeira ou um agente de uma potência estrangeira. *Ver* 50 U.S.C. §§ 1805, 1824.

— A *FREEDOM Act* dos EUA de 2015 alterou o título IV da FISA, que autoriza a utilização de dispositivos de registo de chamadas telefónicas e comunicações eletrónicas, nos termos de uma decisão judicial (exceto em casos urgentes), para exigir que o governo baseie os pedidos num «termo de seleção específico». *Ver* 50 U.S.C. § 1842(c)(3).

— O título V da FISA, que permite ao *Federal Bureau of Investigation* (FBI) obter determinados tipos de documentação empresarial, implica uma decisão judicial com base num pedido que especifique que «existem factos específicos e articuláveis que justificam a convicção de que o cidadão a quem a documentação diz respeito é uma potência estrangeira ou um agente de uma potência estrangeira». *Ver* 50 U.S.C. § 1862(b)(2)(B) ([1])

— Por último, a secção 702 da FISA autoriza que se visem pessoas que se acredite estarem localizadas fora dos Estados Unidos a fim de obter informações no estrangeiro. *Ver* 50 U.S.C. § 188la(a). Assim, como observou a *Privacy and Civil Liberties Oversight Board*, a recolha de dados pelo governo nos termos da secção 702 da FISA «consiste inteiramente em visar cidadãos individuais e obter comunicações associadas a esses cidadãos, dos quais o governo tem motivos para esperar que obterá determinados tipos de informações estrangeiras», pelo que o «programa não funciona através da recolha de comunicações em larga escala». *Privacy and Civil Liberties Oversight Board, Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* (2 de julho de 2014) ([2]).

No que diz respeito às *National Security Letters*, a *FREEDOM Act* de 2015 impõe um requisito de «termo de seleção específico» para a sua utilização. *Ver* 12 U.S.C. § 3414(a)(2); 15 U.S.C. § 1681u; 15 U.S.C. § 1681v(a); 18 U.S.C. § 2709 (b).

Além disso, o *Executive Order 14086* prevê que «[d]eve ser dada prioridade à recolha seletiva» e que, sempre que o setor das informações efetuar a recolha em larga escala, a «recolha em larga escala de informação de origem eletromagnética deve ser autorizada apenas com base numa decisão [...] de que a informação necessária para promover uma prioridade em matéria de informações validada não pode ser razoavelmente obtida através da recolha seletiva». *Ver Executive Order 14086*, § 2(c)(ii)(A).

Além disso, quando o setor das informações determina que a recolha em larga escala satisfaz estas normas, o *Executive Order 14086* prevê garantias adicionais. Especificamente, o decreto executivo exige que o setor das informações, aquando da recolha em larga escala, «aplique métodos e medidas técnicas razoáveis para limitar os dados recolhidos apenas ao necessário para promover uma prioridade em matéria de informações validada, minimizando simultaneamente a recolha de informações que não são pertinentes». *Ver* id., o decreto também enuncia que as «atividades de informação de origem eletromagnética», que incluem a consulta de informação de origem eletromagnética obtida através da recolha em larga escala, «só são realizadas após uma decisão baseada numa avaliação razoável de todos os fatores pertinentes, de que as atividades são necessárias para promover uma prioridade em matéria de informações validada». *Ver id.* § 2(a)(ii)(A). O decreto aplica ainda este princípio afirmando que o setor das informações só pode consultar informação de origem eletromagnética não minimizada obtida em larga escala na consecução de seis objetivos permitidos e que essas consultas devem ser efetuadas de acordo com as políticas e os procedimentos que «tenham em devida conta o impacto [das consultas] na privacidade e nas liberdades cívicas de todos os cidadãos, independentemente da sua nacionalidade ou do local onde residam». *Ver id.* § 2(c)(iii)(D). Por último, o decreto prevê controlos de tratamento, segurança e acesso aos dados recolhidos. *Ver id.* § 2(c)(iii)(A) and§ 2(c)(iii)(B).

* * * * *

Esperamos que estes esclarecimentos sejam úteis. Não hesite em contactar-nos se tiver mais perguntas sobre a forma como o setor norte-americano das informações planeia aplicar o *Executive Order 14086*.

([1]) De 2001 a 2020, o título V da FISA permitiu ao FBI obter autorização junto do FISC para recolher «coisas tangíveis» pertinentes para determinadas investigações autorizadas. Ver USA PATRIOT Act, Pub. L. N.º 107-56, 115 Stat. 272, § 215 (2001). Esta redação, que prescreveu e, por conseguinte, deixou de ser lei, proporcionou a autoridade por intermédio da qual o governo recolheu, em determinado momento, metadados telefónicos em larga escala. No entanto, mesmo antes de a disposição prescrever, a *FREEDOM Act* dos EUA alterou-a para exigir que o governo baseasse um pedido ao FISC num «termo de seleção específico». *Ver* USA Freedom Act de 2015, Pub. L. N.º 114-23, 129 Stat. 268, § I 03 (2015).

([2]) As secções 703 e 704, que autorizam o setor das informações a visar cidadãos norte-americanos localizados no estrangeiro, implicam uma decisão judicial (exceto em casos urgentes) e exigem sempre uma causa provável para considerar que o alvo é uma potência estrangeira, um agente de uma potência estrangeira ou um funcionário ou empregado de uma potência estrangeira. *Ver 50 U.S.C.* §§ 1881b, 1881c.

Sincerely,

Christopher C. FONZONE,
Conselheiro-geral

ANEXO VIII

Lista de abreviaturas

A presente decisão usa as seguintes abreviaturas:

AAA	American Arbitration Association
Regulamento AG	Regulamento relativo ao *Data Protection Review Court* do *Attorney Geral*
AGG-DOM	*Attorney General Guidelines for Domestic FBI Operations* (Orientações do Attorney General sobre as operações nacionais do FBI)
APA	Administrative Procedure Act
CIA	Central Intelligence Agency
CNSS	Committee on National Security Systems
Tribunal de Justiça	Tribunal de Justiça da União Europeia
Decisão	Decisão de Execução da Comissão nos termos do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho sobre a adequação do nível de proteção dos dados pessoais no âmbito Quadro de Privacidade de Dados UE-EUA
DHS	Department of Homeland Security
DNI	Diretor dos Serviços Nacionais de Informações
DoC	*Department of Commerce* dos EUA
DoJ	*Department of Justice* dos EUA
DoT	*Department of Transportation* dos EUA
APD	Autoridade responsável pela Proteção de Dados
Lista QPD	Lista do Quadro de Privacidade de Dados
DPRC	Data Protection Review Court
ECOA	Equal Credit Opportunity Act
ECPA	Electronic Communications Privacy Act
EEE	Espaço Económico Europeu
EO 12333	*Executive Order 12333 «United States Intelligence Activities»* (Decreto Presidencial 12333, Atividades de informação dos Estados Unidos)
EO 14086, EO	*Executive Order 14086 «Enhancing Safeguards for US Signals Intelligence Activities»* (Decreto Presidencial14086, Reforço das salvaguardas para as atividades de recolha de informações de origem eletromagnética dos EUA)
QPD UE-EUA ou QPD	Quadro de Privacidade de Dados UE-EUA
Comité do QPD UE-EUA	Comité do Quadro de Privacidade de Dados UE-EUA
FBI	Federal Bureau of Investigation
FCRA	Fair Credit Reporting Act
FISA	Foreign Intelligence Surveillance Act
FISC	Foreign Intelligence Surveillance Court
FISCR	Foreign Intelligence Surveillance Court of Review
FOIA	Freedom of Information Act
FRA	Federal Records Act

FTC	U.S. Federal Trade Commission
HIPAA	Health Insurance Portability and Accountability Act
ICDR	*International Centre for Dispute Resolution* (Centro Internacional de Resolução de Litígios)
IOB	Intelligence Oversight Board
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSL	National Security Letter(s)
ODNI	Office of the Diretor of National Intelligence
ODNI CLPO, CLPO	*Civil Liberties Protection Officer of the Director of National Intelligence* (CLPO do ODNI)
OMB	Office of Management and Budget
OPCL	Office of Privacy and Civil Liberties of the Department of Justice
PCLOB	Privacy and Civil Liberties Oversight Board
PIAB	President's Intelligence Advisory Board
PPD 28	Presidential Policy Directive 28
Regulamento (UE) 2016/679	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
SAOP	Senior Agency Official for Privacy
Os Princípios	Princípios do Quadro de Privacidade de Dados UE-EUA
US	Estados Unidos
União	União Europeia