COMISSÃO
EUROPEIA

Bruxelas, 12.7.2016
C(2016) 4176 final

DECISÃO DE EXECUÇÃO DA COMISSÃO

de 12.7.2016

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

(Texto relevante para efeitos do EEE)

DECISÃO DE EXECUÇÃO DA COMISSÃO

de 12.7.2016

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

(Texto relevante para efeitos do EEE)

A COMISSÃO EUROPEIA,

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

Tendo em conta a Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados[1], nomeadamente, do artigo 25.º, n.º 6,

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

1. Introdução

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

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

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

4) Nos termos do artigo 25.º, n.º 1, da Diretiva 95/46/CE, os Estados-Membros devem estabelecer que a transferência de dados pessoais para um país terceiro só pode realizar-se se o país terceiro em questão assegurar um nível de proteção adequado e as legislações dos Estados-Membros que transpõem outras disposições da diretiva tiverem sido respeitadas antes de efetuada a transferência. A Comissão pode

[1] JO L 281 de 23.11.1995, p. 31.

[2] Ver Parecer 4/2016 sobre o projeto de decisão relativa ao nível de proteção assegurado pelo Escudo de Proteção da Privacidade UE-EUA, publicada em 30.5.2016.

[3] Processo C-362/14, *Maximillian Schrems/Data Protection Commissioner* («*Schrems*»), EU:C:2015:650, n.º 39.

[4] Processo C-553/07, *Rijkeboer*, EU:C:2009:293, n.º 47; Processos apensos C-293/12 e C-594/12, *Digital Rights Ireland e outros*, EU:C:2014:238, n.º 53; Processo C-131/12, *Google Spain e Google*, EU:C:2014:317, n.os 53, 66 e 74.

considerar que um país terceiro assegura tal nível de proteção adequado em virtude da sua legislação nacional ou dos compromissos internacionais que assumiu a fim de proteger os direitos das pessoas. Nesse caso, e sem prejuízo da observância das disposições nacionais adotadas nos termos de outras disposições da diretiva, os dados pessoais podem ser transferidos dos Estados-Membros sem que sejam necessárias garantias adicionais.

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

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

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

8) Com base nos elementos de prova recolhidos pela Comissão, designadamente nas informações decorrentes dos trabalhos desenvolvidos pelo grupo de contacto UE-EUA sobre a proteção da vida privada[8] e nas informações sobre os programas de informações dos EUA recebidas no grupo de trabalho *ad hoc* UE-EUA[9], a Comissão formulou 13 recomendações para uma reapreciação do sistema «porto seguro». Estas recomendações centraram-se no reforço dos princípios materiais de proteção da privacidade, através no aumento da transparência das políticas de proteção da vida

---

5 Decisão 2000/520/CE da Comissão, de 26 de julho de 2000, nos termos da Diretiva 95/46/CE do Parlamento Europeu e do Conselho e relativa ao nível de proteção assegurado pelos princípios de «porto seguro» e pelas respetivas questões mais frequentes (FAQ) emitidos pelo *Department of Commerce* (equivalente a Ministério do Comércio) dos Estados Unidos da América (JO L 215 de 28.8.2000, p. 7).

6 Comunicação da Comissão ao Parlamento Europeu e ao Conselho Restabelecer a confiança nos fluxos de dados entre a UE e os EUA, COM(2013) 846 final de 27.11.2013.

7 Comunicação da Comissão ao Parlamento Europeu e ao Conselho sobre o funcionamento do sistema «porto seguro» na perspetiva dos cidadãos da UE e das empresas estabelecidas na UE, COM(2013) 847 final de 27.11.2013.

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

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

privada das empresas autocertificadas dos EUA, de uma melhor supervisão, do controlo e da aplicação, pelas autoridades dos EUA, da observância desses princípios, da disponibilidade de mecanismos de resolução de litígios acessíveis, e na necessidade de assegurar que a utilização da derrogação por motivos de segurança nacional constante da Decisão 2000/520/CE da Comissão é proporcionada e se limita ao estritamente necessário.

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

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

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

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

13) A Comissão analisou cuidadosamente a legislação e a prática dos EUA, nomeadamente estes compromissos e declarações oficiais. Com base nas conclusões estabelecidas nos considerandos (136)-(140), a Comissão conclui que os EUA

---

10 [10]Ver nota de rodapé 3.

11 *Schrems*, n.º 97.

12 *Schrems*, n.os 73 e 74.

13 *Schrems*, n.os 88 e 89.

asseguram um nível de proteção adequado dos dados pessoais transferidos ao abrigo do Escudo de Proteção da Privacidade UE-EUA da União para organizações autocertificadas nos Estados Unidos.

2. O «Escudo de Proteção da Privacidade UE-EUA»

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

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

---

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

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

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

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

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

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

2.1. Princípios de privacidade

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

20) No âmbito do *princípio de aviso*, as organizações são obrigadas a fornecer informações aos titulares de dados sobre vários elementos-chave relacionados com o tratamento dos seus dados pessoais (por exemplo, tipo de dados recolhidos, finalidade

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

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

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

do tratamento, direito de acesso e escolha, condições de transferência ulterior e responsabilidade). São aplicáveis garantias adicionais, nomeadamente o requisito de as organizações publicarem as respetivas políticas em matéria de proteção da vida privada (refletindo os princípios), bem como de apresentarem ligações para o sítio Web do *Department of Commerce* (com informações adicionais sobre a autocertificação, os direitos dos titulares de dados e os mecanismos de recursos disponíveis), a lista do Escudo de Proteção da Privacidade (a que se refere o considerando 30) e o sítio Web de uma entidade adequada de resolução alternativa de litígios.

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

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

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

24) No âmbito do *princípio de segurança*, as organizações que criam, mantêm, utilizam ou divulgam dados pessoais devem tomar precauções de segurança «razoáveis e adequadas», tomando em consideração os riscos que o tratamento e a natureza dos

---

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

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

dados implicam. No caso de tratamento ulterior, as organizações devem celebrar um contrato com a entidade que procederá ao tratamento ulterior dos dados que assegure o mesmo nível de proteção previsto pelos princípios e tomar medidas para assegurar a sua aplicação adequada.

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

26) No âmbito do *princípio de recurso, aplicação e responsabilidade*,[25] as organizações participantes devem proporcionar mecanismos robustos para assegurar a conformidade com os restantes princípios e vias de recurso para todos os titulares de dados cujos dados pessoais tenham sido tratados de modo não conforme, nomeadamente reparações eficazes. Quando uma organização tenha decidido, a título voluntário, autocertificar[26] a sua adesão ao Escudo de Proteção da Privacidade UE-EUA, o cumprimento efetivo dos princípios é obrigatório. Para poder continuar a basear-se no Escudo de Proteção da Privacidade para receber dados pessoais da União, as

---

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

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

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

25 Ver igualmente o princípio suplementar «Resolução de litígios e aplicação» (Secção III.11. do anexo II).

26 Ver igualmente o princípio suplementar «Autocertificação» (Seção III.6 do anexo II).

organizações devem proceder anualmente à certificação da sua participação no quadro. As organizações devem também tomar medidas para verificar[27] que as suas políticas públicas em matéria de proteção da vida privada são conformes com os princípios de privacidade e são efetivamente cumpridas. Tal pode ser efetuado através de um sistema de autoavaliação, que deve incluir procedimentos internos que assegurem que os trabalhadores recebem formação sobre a aplicação das políticas da organização em matéria de proteção da vida privada e que a conformidade é periodicamente reexaminada de forma objetiva, ou verificações de conformidade externas, cujos métodos podem incluir auditorias ou verificações aleatórias. Além disso, a organização deve criar um mecanismo de recurso efetivo para tratar eventuais queixas (ver igualmente a este respeito o considerando 43) e estar sujeita aos poderes de investigação e de execução da FTC, do *Department of Transportation* e de qualquer outro organismo oficial americano que assegurará o respeito efetivo dos princípios.

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

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

---

27 Ver igualmente o princípio suplementar «Verificação» (Seção III.7 do anexo II).

28 Ver igualmente o princípio suplementar «Contratos obrigatórios para as transferências posteriores» (Secção III.10. do anexo II).

29 Ver igualmente o princípio suplementar «Contratos obrigatórios para as transferências posteriores» (Secção III.10.b do anexo II). Embora este princípio autorize igualmente transferências que assentem em instrumentos não contratuais (por exemplo, programas de conformidade e controlo intragrupo), o texto indica claramente que esses instrumentos devem sempre «garantir a continuidade da proteção das informações pessoais em conformidade com os princípios». Além disso, dado que a organização americana autocertificada continuará a ser responsável pelo respeito do princípio, terá todo o interesse em utilizar instrumentos realmente eficazes na prática.

30 Ver a secção I.5. do anexo II.

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

integridade dos dados e limitação dos fins, a obrigação de fornecer o mesmo nível de proteção que o garantido pelos princípios, pressupõe que o terceiro só pode tratar as informações pessoais que lhe foram transmitidas para fins que não sejam incompatíveis com os as finalidades para as quais foram inicialmente recolhidos ou posteriormente autorizados pelo titular dos dados.

29) A obrigação de fornecer o mesmo nível de proteção que o garantido pelos princípios é aplicável a todos os terceiros que intervenham no tratamento dos dados assim transferidos independentemente da sua localização (nos EUA ou num outro país terceiro), bem como quando o destinatário terceiro inicial comunica por sua vez esses dados a um outro destinatário terceiro, por exemplo, para fins de subcontratação. De qualquer modo, o contrato com o destinatário terceiro deve prever que, se este último verificar que deixou de estar em condições de cumprir esta obrigação, informará do facto a organização aderente ao Escudo de Proteção da Privacidade. Nesse caso, deve pôr termo ao tratamento ou devem ser tomadas outras medidas razoáveis e adequadas para solucionar a situação[32]. Sempre que surjam problemas de cumprimento na cadeia de (sub)tratamento, a organização aderente ao Escudo de Proteção da Privacidade agindo como responsável pelo tratamento dos dados pessoais deverá provar que não é responsável pela questão que dá origem aos danos; caso contrário deverá assumir a responsabilidade, em conformidade com o *princípio de recurso, aplicação e responsabilidade*. Estão previstas proteções suplementares em caso de transferência posterior para um mandatário terceiro[33].

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

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

31) Para que o Escudo de Proteção da Privacidade UE-EUA seja corretamente aplicado, as partes interessadas, tal como os titulares dos dados, os exportadores de dados e as autoridades nacionais responsáveis pela proteção dos dados devem estar em condições de identificar as organizações aderentes aos princípios. Para o efeito, o *Department of Commerce* assumiu a responsabilidade de manter atualizada e disponibilizar ao público uma lista das organizações que autocertificaram a sua adesão aos princípios e que estão abrangidas pelo âmbito de competência de, pelo menos, uma das autoridades de execução referidas nos anexos I e II da presente decisão («lista do Escudo de

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

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

Proteção da Privacidade»)[34]. O *Department of Commerce* atualizará a lista com base nos pedidos de renovação da certificação anual das organizações e sempre que uma organização se retire ou seja suprimida do Escudo de Proteção da Privacidade UE-EUA. Também conservará e disponibilizará ao público um registo oficial das organizações suprimidas da lista que, em cada caso, identifica o motivo de tal supressão. Por último, fornecerá uma ligação para a lista de processos da FTC relacionados com a aplicação do Escudo de Proteção da Privacidade conservados que figurará no sítio Web da FTC.

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

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

34) Além disso, o *Department of Commerc*e procederá ao controlo das organizações que já não participam no Escudo de Proteção da Privacidade UE-EUA, quer por se terem retirado voluntariamente ou por a sua certificação ter caducado, a fim de verificar se devolverão, eliminarão ou manterão[35] os dados pessoais previamente recebidos no âmbito do quadro. Se mantiverem estes dados, as organizações são obrigadas a aplicar-lhes os princípios. Nos casos em que o *Department of Commerce* tenha afastado organizações do quadro devido ao incumprimento persistente dos princípios, esta entidade certificar-se-á de que as referidas organizações devolvem ou eliminam os dados pessoais recebidos no âmbito do quadro.

35) Sempre que, por algum motivo, uma organização abandone o Escudo de Proteção da Privacidade UE-EUA, esta deve eliminar todas as declarações públicas que sugiram que continua a participar no mesmo ou que tem direito aos seus benefícios, nomeadamente quaisquer referências ao Escudo de Proteção da Privacidade UE-EUA na sua política pública em matéria de proteção da vida privada. O *Department of*

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

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

Commerce procurará e resolverá as falsas declarações de participação no Escudo, incluindo por parte de antigos participantes[36]. Todas as falsas declarações destinadas ao grande público relativamente à adesão aos princípios sob a forma de declarações ou práticas enganosas são passíveis de medidas de execução pela FTC, pelo *Department of Transportation* ou por outras autoridades de execução americanas; as declarações falsas prestadas ao *Department of Commerce* são passíveis de execução ao abrigo do *False Statements Act* (legislação sobre falsas declarações — 18 USC § 1001)[37].

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

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

2.3. Mecanismo de recurso, tratamento de queixas e execução

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

39) No quadro da sua autocertificação, as organizações devem satisfazer os requisitos do princípio de recurso, aplicação e responsabilidade, prevendo mecanismos de recurso

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

independentes facilmente acessíveis e eficazes, através dos quais as queixas e os litígios possam ser examinados e resolvidos sem custos para os titulares de dados.

40) As organizações podem escolher mecanismos de recurso independentes na União ou nos Estados Unidos, opção que inclui a possibilidade de se comprometer, numa base voluntária, a cooperar com as autoridades responsáveis pela proteção de dados (APD) da UE. Todavia, uma tal escolha não existe quando as organizações tratam dados relativos aos recursos humanos, uma vez que nesse caso a cooperação com as APD é obrigatória. Outras alternativas consistem em recorrer a um organismo independente de resolução alternativa de litígios ou a *programas de proteção da privacidade* elaborados pelo setor privado, que integram os princípios nas suas regras. Estes devem incluir mecanismos de execução eficazes conformes aos requisitos do princípio de recurso, aplicação e responsabilidade. As organizações são obrigadas a solucionar os problemas de não conformidade. Devem igualmente especificar que estão sujeitas aos poderes de investigação e de execução da FTC, do *Department of Transportation* ou de qualquer outro organismo oficial americano.

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

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

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

44) Após a receção de uma queixa individual, independentemente de ser apresentada diretamente pelo interessado ou através do *Department of Commerce* na sequência de um reenvio por uma APD, a organização deve fornecer uma resposta ao titular de dados da UE num prazo de 45 dias. Esta resposta deve incluir uma apreciação do mérito da queixa e informações sobre a maneira como a organização resolverá o problema. Do mesmo modo, as organizações devem responder rapidamente às questões e a outros pedidos de informação relativos à sua adesão aos princípios que

lhes são dirigidos pelo *Department of Commerce* ou por uma APD[39] (quando a organização se comprometeu a cooperar com a APD). As organizações devem conservar arquivos sobre a execução das suas políticas de privacidade e disponibilizá-los, mediante pedido, a uma instância de recurso independente ou à FTC (ou a outra autoridade dos EUA com competência para investigar práticas desleais e enganosas), no quadro de uma investigação ou de uma queixa por não conformidade.

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

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

47) Nos casos em que a organização não cumpra a decisão de um organismo de autorregulação ou de resolução de litígios, este último deve notificar o incumprimento ao *Department of Commerce* e à FTC (ou a outra autoridade dos EUA com competência para investigar práticas desleais e enganosas), ou a um tribunal competente[41]. Se uma organização se recusar a cumprir uma decisão definitiva de um organismo de autoregulação, um organismo independente de resolução de conflitos, ou um organismo público competente em matéria de privacidade, ou quando o referido organismo determinar que uma organização não cumpre frequentemente os princípios, tal será considerado como um incumprimento sistemático o que implica que o *Department of Commerce*, após dar à organização que não cumpriu um pré-aviso de 30 dias e uma oportunidade para responder, eliminará a referida organização da lista[42]. Se, uma vez suprimida da lista, a organização continuar a alegar a sua certificação de

---

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

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

[41] Ver a secção III.11.e. do anexo II.

[42] Ver a secção III.11.g. do anexo II, em especial os pontos ii) e iii).

participação no Escudo de Proteção da Privacidade, o *Department of Commerce* submeterá a questão à FTC ou outro organismo com funções coercivas[43].

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

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

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

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

---

43 Ver anexo I, secção sobre «Procura e Resolução de falsas declarações de participação».

44 O regulamento interno do painel informal da APD deve ser estabelecido pelas APD com base na sua competência para organizar o seu trabalho e cooperar entre si.

45 Ver o anexo I, secções sobre «Reforço da cooperação com as APD» e «Facilitar a resolução de queixas por incumprimento», bem como a secção II.7.e. do anexo II.

46 Ver anexo IV, p.6.

47 *ibid*.

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

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

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

55) A FTC pode assegurar a conformidade através de decisões administrativas («injunções») e controlará sistematicamente a conformidade com estas decisões.

---

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

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

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

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

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

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

58) O Comité do Escudo de Proteção da Privacidade terá competência para aplicar as «medidas equitativas, específicas do titular dos dados e não monetárias»[55] necessárias para corrigir o incumprimento dos princípios. Embora o comité tome em consideração

---

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

52 Ver a secção II.1.xi e III.7.c. do anexo II.

53 O número de árbitros no comité deverá ser acordado entre as partes.

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

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

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

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

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

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

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

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

3. Acesso e utilização de dados pessoais, transferidos ao abrigo do Escudo de Proteção da Privacidade UE-EUA, pelas autoridades públicas dos EUA

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

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

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

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

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

3.1.1. Limitações

68) Nos termos da Constituição dos EUA, o Presidente, na qualidade de Comandante Supremo e Chefe do Executivo, é responsável por garantir a segurança nacional e, no que diz respeito às informações externas, é responsável pelos negócios estrangeiros dos EUA[58]. Embora o Congresso tenha competência para impor limitações, e o tenha feito em vários aspetos, o Presidente dentro destes limites pode administrar as

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

[57] Ver *Schrems*, n.º 91.

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

atividades do setor das informações dos EUA, nomeadamente através de decretos executivos ou diretivas presidenciais. Tal é igualmente aplicável aos domínios nos quais não existem orientações do Congresso. Atualmente, os dois instrumentos jurídicos centrais a este respeito são o Decreto Executivo n.º 12333 («E.O. 12333»)[59] e a *Presidential Policy Directive* 28.

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

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

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

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

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

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

70) A PPD-28 estabelece que as informações de origem eletromagnética podem ser recolhidas exclusivamente nos casos em que exista um objetivo de espionagem externa ou de contraespionagem ou para apoiar missões nacionais e departamentais e não para qualquer outro fim (por exemplo, para proporcionar uma vantagem concorrencial às empresas dos EUA). Relativamente a este aspeto, o ODNI explica que os serviços de informações «devem exigir que, sempre que possível, a recolha incida em objetivos ou temas de informação externa específicos através da utilização de discriminantes (por exemplo, mecanismos específicos, termos de seleção e identificadores).»[63] Além disso, as declarações fornecem garantias de que as decisões

---

59 E.O. 12333: *United States Intelligence Activities*, Federal Register Vol. 40, n.º 235 (8.12.1981). Na medida em que o decreto executivo se encontre acessível ao público, este define os objetivos, as orientações, os deveres e as responsabilidades da procura de informações dos EUA (incluindo o papel dos vários elementos do setor das informações) e estabelece os parâmetros gerais de conduta das atividades dos serviços de informações (em especial a necessidade de promulgar regras processuais específicas). Segundo a secção 3.2. do Decreto Executivo n.º 12333, o Presidente, apoiado pelo *National Security Council*, e o DNI devem emitir as diretivas, os procedimentos e orientações adequados necessários para dar cumprimento ao decreto.

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

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

62 Ver Memorando do *Office of Legal Counsel, Department of Justice* (DOJ), ao Presidente Clinton, 29.01.2000. De acordo com este parecer jurídico, as diretivas presidenciais têm o mesmo «efeito jurídico substantivo que um decreto executivo».

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

sobre a recolha de informações não são deixadas à discrição dos agentes dos serviços de informações, estando sujeitas às políticas e aos procedimentos que os vários serviços do setor das informações dos EUA são obrigados a adotar para aplicar a PPD-28[64]. Por conseguinte, a investigação e determinação de seletores adequados ocorre no âmbito do «*National Intelligence Priorities Framework*» (NIPF) (quadro das prioridades dos serviços de informações nacionais — NIPF) que assegura que as prioridades em termos de informações são definidas por decisores políticos de alto nível e regularmente reexaminadas para que continuem a responder às ameaças reais à segurança nacional, tendo em em consideração os possíveis riscos relacionados para a privacidade[65]. Com base no que precede, o pessoal dos serviços de informações investiga e identifica termos de seleção específicos que devem recolher informações externas que dão resposta às prioridades[66]. Os termos de seleção ou «seletores» devem ser regularmente reexaminados para determinar se ainda proporcionam informações valiosas em conformidade com as prioridades[67].

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

72) Embora a PPD-28 explique que os elementos do setor das informações devem, por vezes recolher informação de origem eletromagnética em larga escala em determinadas circunstâncias, por exemplo, para identificar e avaliar ameaças novas ou emergentes, estabelece que esses elementos devem dar prioridade a alternativas que permitam a recolha de informação seletiva de origem eletromagnética[71]. Daqui resulta

---

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

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

66 Declarações do ODNI (anexo VI), p. 6. Ver por exemplo, *NSA Civil Liberties and Privacy Office* (NSA CLPO), *NSA's Civil Liberties and Privacy Protections for Targeted SIGINT Activities under Executive Order* 12333, 7.10.2014. Ver também o relatório de situação do ODNI relativo a 2014. No que se refere aos pedidos de acesso ao abrigo da secção 702 da FISA, as questões são regidas pelos procedimentos de minimização aprovados pelo FISC. Ver NSA CLPO, *NSA's Implementation of Foreign Intelligence Surveillance Act Section* 702, 16.4.2014.

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

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

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

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

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

que a recolha em larga escala só será autorizada quando a recolha seletiva através da utilização de discriminantes - isto é, identificadores associados a um objetivo específico (como o correio eletrónico ou o número do telefone do objetivo)- não possa realizar-se por motivos técnicos ou operacionais[72]. O que precede é aplicável à forma de recolha da informação de origem eletromagnética e ao conteúdo que é efetivamente recolhido[73].

73) Segundo as declarações da ODNI, mesmo quando os serviços de informações não puderem utilizar identificadores específicos para especificar a recolha, aqueles procurarão reduzir a recolha «tanto quanto possível». Para garantir isto, «aplicarão filtros e outras ferramentas técnicas para centrar a recolha nas instalações suscetíveis de conter comunicações com valor para as informações externas» (dando assim resposta a requisitos dos responsáveis políticos dos Estados Unidos no que diz respeito ao procedimento descrito no ponto 70). Como consequência deste facto, a recolha em larga escala centrar-se-á, pelo menos, de duas maneiras: em primeiro lugar, dirá sempre respeito a objetivos específicos de informações externas (por exemplo, adquirir informação de origem eletromagnética sobre as atividades de um grupo terrorista que opera numa determinada região) e centrar a recolha em comunicações que possuem esse nexo. Segundo a garantia dada pelo ODNI, tal reflete-se no facto de as atividades de informação de origem eletromagnética dos Estados Unidos se referirem apenas a uma fração das comunicações através da Internet[74]. Em segundo lugar, as declarações do ODNI explicam que os filtros e outros instrumentos técnicos utilizados serão concebidos para centrará a recolha «da forma mais exata possível», a fim de garantir que a quantidade de «informação não pertinente» recolhida seja mínima.

74) Por último, mesmo nos casos em que os Estados Unidos consideram necessário efetuar a recolha em grande escala de informação de origem eletromagnética, nas condições estabelecidas nos considerandos 70-73, a PPD-28 limita a utilização desta informação a uma lista específica de seis objetivos de segurança nacional com vista a proteger a privacidade e as liberdades cívicas de todas as pessoas, independentemente da sua nacionalidade ou local de residência[75]. Estes objetivos admissíveis englobam medidas de deteção e combate a ameaças decorrentes de espionagem, terrorismo, armas de destruição maciça, ameaças à cibersegurança, para as forças armadas ou o pessoal militar, bem como ameaças criminosas transnacionais relacionadas com os restantes cinco objetivos e serão reexaminados, pelo menos, anualmente. De acordo com as declarações do governo dos EUA, os elementos do setor das informações reforçaram as suas normas e práticas analíticas para a consulta de informação de origem eletromagnética não avaliada a fim de cumprir estes requisitos; a utilização de consultas seletivas «assegura que apenas os elementos que se consideram deter um potencial valor informativo são apresentados aos analistas para efeitos de análise».[76]

75) Estas limitações são de especial relevância para os dados pessoais transferidos ao abrigo do Escudo de Proteção da Privacidade, nomeadamente se a recolha de dados

---

um software alternativo que substitua na íntegra a recolha em larga escala na deteção de algumas ameaças para a segurança nacional». Ver *Signals Intelligence Reform, 2015 Anniversary Report*.

72 Ver declarações do ODNI (anexo VI), p. 3.

73 Declarações do ODNI (anexo VI), p. 3.

74 Declarações do ODNI (anexo VI). Isto aborda especificamente a preocupação expressa pelas autoridades nacionais de proteção de dados no seu parecer sobre o projeto de decisão de adequação. Ver o Parecer 1/2016 do grupo de trabalho do artigo 29.º sobre a proteção de dados, sobre o projeto de decisão de adequação sobre o Escudo de Proteção da Privacidade UE-EUA (adotado em 13.4.2016), p. 38, n.º 47.

75 Ver secção 2 da PPD-28.

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

pessoais ocorrer fora dos Estados Unidos da América, designadamente durante o seu trânsito nos cabos transatlânticos da União para os Estados Unidos. Tal como confirmado pelas autoridades dos EUA nas declarações do ODNI, as limitações e garantias aí estabelecidas — designadamente as da PPD-28 — são aplicáveis a tal recolha[77].

76) Embora não enunciados nesses termos jurídicos, estes princípios refletem a essência dos princípios de necessidade e proporcionalidade. É evidentemente atribuída prioridade à recolha seletiva, ao passo que a recolha em larga escala é limitada a situações (excecionais) nas quais a recolha seletiva não é possível por motivos técnicos ou operacionais. Mesmo nos casos em que não seja possível evitar a *recolha em larga escala*, a «utilização» posterior de tais dados através do acesso é *estritamente limitada* a objetivos de segurança nacional específicos e legítimos[78].

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

78) Decorre das informações disponíveis, nomeadamente das declarações recebidas do governo dos EUA, que após a transferência dos dados para organizações localizadas nos Estados Unidos e autocertificadas ao abrigo do Escudo de Proteção da Privacidade UE-EUA, os serviços de informações dos EUA só podem[79] solicitar dados pessoais nos casos em que o seu pedido respeite a *Foreign Intelligence Surveillance Act* (lei relativa à vigilância dos serviços de informações externas— FISA) ou seja efetuado pelo *Federal Bureau of Investigation* (FBI) (Gabinete Federal de Investigação) com base numa denominada *National Security Letter* (carta de segurança nacional — NSL)[80]. Existem várias bases jurídicas ao abrigo da FISA que podem ser utilizadas para recolher (e subsequentemente tratar) os dados pessoais de titulares de dados da UE transferidos no âmbito do Escudo de Proteção da Privacidade UE-EUA. Para além da secção 104 da FISA[81] que abrange vigilância eletrónica individualizada tradicional

---

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

78 Ver *Schrems*, n.º 93.

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

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

81 50 U.S.C. § 1804. Não obstante o facto de esta autoridade jurídica exigir uma «declaração dos factos e circunstâncias subjacentes ao pedido do requerente para justificar a sua convicção de que a) o alvo da vigilância eletrónica é uma potência estrangeira ou um agente de uma potência estrangeira», este último pode incluir cidadãos de países terceiros envolvidos em terrorismo internacional ou na proliferação internacional de armas de destruição maciça (incluindo atos preparatórios) (50 U.S.C. § 1801 (b)(1)). Contudo, existe apenas uma ligação teórica aos dados pessoais transferidos ao abrigo do Escudo de Proteção

e da secção 402 da FISA[82] e da instalação de dispositivos de registo de chamadas telefónicas e comunicações eletrónicas, os dois instrumentos centrais são a secção 501 da FISA (antiga secção 215 da *U.S. PATRIOT ACT*) e a secção 702 da FISA[83].

79) A este respeito, a *USA FREEDOM Act*, adotada em 2 de junho de 2015, proíbe a recolha em larga escala de registos com base na secção 402 da FISA (autoridade em matéria de dispositivos de registo de chamadas telefónicas e comunicações eletrónicas), na secção 501 da FISA (antiga secção 215 da Patriot Act)[84] e através da utilização de NSL e, em vez disso, exige a utilização de «termos de seleção» específicos[85].

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

81) Tal é evidente no que se refere à vigilância eletrónica individualizada tradicional nos termos da secção 104 da FISA[86]. Relativamente à secção 702 da FISA, que constitui a base de dois programas de informações importante geridos pelos serviços de informações dos EUA (PRISM, UPSTREAM), as investigações são realizadas de forma seletiva através da utilização de seletores individuais que identificam meios de comunicação específicos, tais como o endereço eletrónico ou o número de telefone da pessoa visada, mas não palavras-chave nem mesmo os nomes das pessoas em causa[87].

---

da Privacidade UE-EUA, uma vez que a declaração dos factos também deve justificar a convicção de que «cada um dos locais ou meios de comunicação que são alvos da vigilância eletrónica estão a ser utilizados, ou serão em breve utilizados, por uma potência estrangeira ou um agente de uma potência estrangeira». De qualquer modo, a utilização desta autoridade exige a apresentação de um pedido ao FISC que avaliará, entre outras questões, se, com base nos factos apresentados, existe uma causa provável de que tal se verifique efetivamente.

82 50 U.S.C. § 1842 com § 1841(2) e secção 3127 do título 18. Esta autoridade não diz respeito ao conteúdo das comunicações, visando, em vez disso, as informações sobre o cliente ou assinante que utiliza um serviço (tais como nome, endereço, número de cliente, duração/tipo de serviço recebido, fonte/mecanismo de pagamento). O que precede exige o pedido de uma decisão emitida pelo FISC (ou por um magistrado dos EUA) e a utilização de um termo de seleção específico na aceção de § 1841(4), isto é, um termo que identifique especificamente, por exemplo, uma pessoa ou conta e seja utilizado para limitar, tanto quanto razoavelmente possível, o âmbito da informação procurada.

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

84 Com base nesta disposição, o FBI pode solicitar «coisas tangíveis» (por exemplo, registos e documentação) com base numa demonstração ao *Foreign Intelligence Surveillance Court* (tribunal encarregado de supervisionar os pedidos e mandatos em matéria de vigilância — FISC) de que existem motivos razoáveis para considerar que são relevantes para uma investigação específica do FBI. Na realização da sua investigação, o FBI deve utilizar termos de seleção aprovados pelo FISC relativamente aos quais exista uma «suspeita razoável e articulável» de que tal termo se encontra associado a uma ou mais potências estrangeiras ou aos seus agentes envolvidos em terrorismo internacional ou atividades de preparação do mesmo. Ver PCLOB, Sec. 215 Report, p. 59; *NSA CLPO, Transparency Report*: *The USA Freedom Act Business Records FISA Implementation*, 15.1.2016, pp. 4-6.

85 Declarações do ODNI (anexo VI), p. 13 (n.º 38).

86 Ver nota de rodapé 81.

87 PCLOB, Sec. 702 *Report*, pp. 32-33 com referências adicionais. De acordo com o seu serviço de proteção da vida privada, a NSA deve verificar se existe uma relação entre o alvo e o seletor, deve documentar as

Portanto, tal como referido pela *Privacy and Civil Liberties Oversight Board* (comissão de controlo da privacidade e das liberdades cívicas — PCLOB), a vigilância da secção 702 «consiste exclusivamente em visar cidadãos [de países terceiros] específicos sobre os quais foi feita uma determinação individualizada»[88]. Devido a uma cláusula de «caducidade», será necessário rever a secção 702 da FISA em 2017, data em que a Comissão terá de reexaminar as garantias à disposição dos titulares de dados da UE.

82) Além disso, nas suas declarações, o governo dos EUA apresentou garantias explícitas à Comissão Europeia de que o setor das informações dos EUA «não procede à vigilância indiscriminada de ninguém, nomeadamente de cidadãos europeus comuns»[89]. No que diz respeito aos dados pessoais recolhidos nos EUA, esta declaração é apoiada por dados empíricos que demonstram que os *pedidos de acesso* através de NSL e nos termos da FISA, tanto a nível individual como em conjunto, dizem respeito a um número relativamente reduzido de alvos quando comparados com o fluxo global de dados na Internet[90].

83) No que se refere ao *acesso* a dados recolhidos e à *segurança dos dados*, a PPD-28 exige que o acesso seja «limitado ao pessoal autorizado com necessidade de conhecer as informações para desempenhar a sua missão» e que as informações pessoais «devem ser tratadas e armazenadas em condições que proporcionem uma proteção adequada e impeçam o acesso de pessoas não autorizadas, em conformidade com as garantias aplicáveis às informações sensíveis». O pessoal dos serviços de informações recebe formação apropriada e adequada sobre os princípios estabelecidos na PPD-28[91].

---

informações no estrangeiro que prevê obter, estas informações devem ser revistas e aprovadas por dois analistas principais da NSA e o processo global será rastreado para subsequentes verificações de conformidade pelo ODNI e o Department of Justice. Ver *NSA CLPO, NSA's Implementation of Foreign Intelligence Act Section 702*, 16.4.2014.

88 PLCOB, Sec. 702 Report, p. 111. Ver também declarações do ODNI (anexo VI), p. 9 («a recolha nos termos da secção 702 da [FISA] não é maciça e indiscriminada», incidindo estreitamente sobre a recolha de informações externas de alvos legítimos e individualmente identificados) e p. 13, n.º 36 (com referência a um parecer de 2014 do FISC); NSA CLPO, NSA's *Implementation of Foreign Intelligence Act Section* 702, 16.4.2014. Mesmo no caso do programa UPSTREAM, a NSA só pode solicitar a interceção de comunicações eletrónicas de, para ou sobre seletores atribuídos.

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

90 Ver *Statistical Transparency Report Regarding Use of National Security Authorities*, 22.4.2015. No que se refere ao fluxo global de dados na Internet, ver, por exemplo, *Fundamental Rights Agency, Surveillance by Intelligence Services*: Direitos fundamentais, salvaguardas e recursos na UE (2015), pp. 15-16. No respeitante ao programa UPSTREAM, segundo um parecer desclassificado do FISC de 2011, mais de 90 % das comunicações eletrónicas obtidas nos termos da secção 702 da FISA são provenientes do programa PRISM, ao passo que menos de 10 % são provenientes do programa UPSTREAM. Ver *FISC, Memorandum Opinion*, 2011 WL 10945618 (FISA Ct., 3.10.2011), n.º 21 (disponível em: http://www.dni.gov/files/documents/0716/October-2011-Bates-Opinion-and%20Order-20140716.pdf).

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

84) Por último, no que se refere à *conservação* e posterior *divulgação* de dados pessoais de titulares de dados da UE recolhidos pelos serviços de informações dos EUA, a PPD-28 estabelece que todas as pessoas (incluindo cidadãos de países terceiros) devem ser tratadas com dignidade e respeito, que todas as pessoas têm interesses legítimos de privacidade no tratamento dos seus dados pessoais e que os elementos do setor das informações devem, portanto, criar políticas que proporcionem garantias adequadas para os referidos dados «razoavelmente concebidas para minimizar o [seu] risco de divulgação e preservação»[92].

85) O governo dos EUA explicou que este requisito de razoabilidade significa que os elementos do setor das informações não terão de adotar «todas as medidas teoricamente possíveis», mas terão de «equilibrar os seus esforços para proteger os interesses legítimos em matéria de privacidade e liberdades cívicas com as necessidades práticas das atividades de informação de origem eletromagnética».[93] A este respeito, os cidadãos de países terceiros serão tratados do mesmo modo que os cidadãos dos EUA, com base nos procedimentos aprovados pelo *Attorney General*[94].

86) De acordo com estas regras, em geral, a preservação limita-se a um período máximo de cinco anos, a menos que exista uma determinação específica na legislação ou uma determinação expressa efetuada pelo *Director of National Intelligence* após uma avaliação cuidadosa das preocupações em matéria de privacidade — tomando em consideração as opiniões do *Civil Liberties Protection Officer* (agente responsável pela proteção das liberdades cívicas) do ODNI, bem como dos funcionários responsáveis pela proteção da privacidade e das liberdades cívicas — de que a preservação continuada é do interesse da segurança nacional[95]. A divulgação limita-se aos casos nos quais as informações são relevantes para o objetivo subjacente à recolha e, como tal, dão resposta a um pedido autorizado em matéria de aplicação da lei ou informações externas[96].

---

eletromagnética, os elementos do setor das informações (nomeadamente o FBI, a CIA e a NSA) tomaram medidas para aumentar a sensibilização do seu pessoal para os requisitos da PPD-28 através da criação de novas políticas de formação ou da alteração das políticas existentes.

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

93 Ver declarações do ODNI (anexo VI).

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

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

96 Nomeadamente no caso da secção 501 da FISA (antiga secção 215 da Patriot Act), a divulgação de informações pessoais pode ocorrer apenas para efeitos de luta contra o terrorismo ou como prova de um crime; no caso da secção 702 da FISA, apenas se existir um objetivo válido em matéria de aplicação da lei ou informações externas. Ver *NSA, CLPO, NSA's Implementation of Foreign Intelligence Surveillance Act* Secção 702, 16.4.2014; Transparency Report: *The USA Freedom Act Business Records FISA*

87) De acordo com as garantias oferecidas pelo governo dos EUA, as informações pessoais não podem ser divulgadas exclusivamente porque o titular dos dados é um cidadão de um país terceiro e «a informação de origem eletromagnética sobre as atividades quotidianas de um estrangeiro não seria considerada informação externa passível de divulgação ou preservação permanente por força simplesmente desse facto, a menos que dê resposta de outro modo a um pedido autorizado em matéria de informações externas».[97]

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

89) Tal como o mostrou a análise anterior, o direito americano garante que as medidas de vigilância servirão apenas para a obtenção de informações oriundas do estrangeiro, o que constitui um objetivo estratégico legítimo[98], e serão o mais possível adaptadas. Em especial, a recolha em larga escala só será autorizada a título excecional, quando não for viável uma recolha seletiva, sendo acompanhada de salvaguardas adicionais com vista a limitar ao máximo a quantidade de dados recolhidos e o posterior acesso (que deverá ser centrado e autorizado unicamente para fins específicos).

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

---

Implementation, 15.1.2016. Ver também *NSA's Civil Liberties and Privacy Protections for Targeted SIGINT Activities under Executive Order 12333*, 7.10.2014.

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

98 O Tribunal de Justiça especificou que a segurança nacional constitui um objetivo legítimo. Ver *Schrems*, n.º 88. Ver igualmente o acórdão do Tribunal de Justiça proferido no processo *Digital Rights Ireland and Others*, n.ºs 42-44 e 51, no qual o Tribunal de Justiça considerou que a luta contra as formas graves de criminalidade, em especial a criminalidade organizada e o terrorismo pode depender, numa grande medida, da utilização de técnicas modernas de investigação. Além disso, ao contrário do que se passa nas investigações penais, que tradicionalmente dizem respeito à determinação retroativa da responsabilidade e da culpa por comportamentos passados, as atividades dos serviços de informação incidem frequentemente na prevenção de ameaças à segurança nacional antes de ocorrerem danos. Por conseguinte, a referida investigação pode muitas vezes ter de cobrir uma gama mais vasta de eventuais atores («objetivos») e uma área geográfica mais ampla. Ver TEDH, *Weber and Saravia/Alemanha*, Decisão de 29.6.2006, Pedido n.º 54934/00, pontos 105-118 (sobre o denominado «acompanhamento estratégico»).

99 Acórdão *Schrems*, n.º 91, com referências adicionais.

100 Acórdão *Schrems*, n.º 93.

Internet, excluem que se possa aceder «numa base generalizada»[101] ao conteúdo das comunicações eletrónicas.

3.1.2. Proteção jurídica efetiva

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

Supervisão

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

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

94) Segundo a PPD-28, secção 4(a)(iv), as políticas e os procedimentos dos elementos do setor das informações «devem incluir medidas adequadas para facilitar a supervisão da implementação de garantias que protejam as informações pessoais»; estas medidas devem incluir auditorias periódicas[102].

95) Foram instaurados vários níveis de supervisão a este respeito, nomeadamente os agentes responsáveis pela proteção das liberdades cívicas ou da privacidade, os inspetores-gerais, o *Civil Liberties and Privacy Office* (gabinete responsável pela proteção da privacidade e das liberdades cívicas) do ODNI, a PCLOB e a *Intelligence Oversight Board* (comissão de supervisão dos serviços de informações) do Presidente. Estas funções de supervisão são apoiadas pelo pessoal responsável pela conformidade em todos os serviços[103].

96) Tal como explicado pelo governo dos EUA[104], *os agentes responsáveis pelas liberdades cívicas ou a privacidade* com responsabilidade de supervisão existem em vários departamentos com responsabilidades em matéria de informações e serviços de informações[105]. Embora os poderes específicos destes agentes possam variar um pouco em função do estatuto de autorização, normalmente englobam a supervisão dos procedimentos a fim de assegurar que o respetivo departamento/organismo tem em devida consideração a proteção da privacidade e das liberdades cívicas e instaurou procedimentos adequados para a resolução de queixas de pessoas que consideram que a sua privacidade ou liberdades cívicas foram violadas (e, em alguns casos, como o

---

101 Ver acórdão *Schrems*, n.º 94.

102 ODNI, *Safeguarding the Personal Information of all People*: *A Status Report on the Development and Implementation of Procedures under Presidential Policy Directive 28*, p. 7. Ver, por exemplo, CIA, *Signals Intelligence Activities*, p. 6 (*Compliance*); FBI, *Presidential Policy Directive 28 Policies and Procedures*, Sec. III (A)(4), (B)(4); NSA, PPD-28 *Section 4 Procedures*, 12.1.2015, Sec. 8.1, 8.6(c).

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

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

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

ODNI, podem ter competência para investigar queixas[106]). O chefe do departamento/organismo, por sua vez, deve assegurar que o agente recebe todas as informações e tem acesso a todos os materiais necessários ao desempenho das suas funções. Os agentes responsáveis pela proteção da privacidade e das liberdades cívicas comunicam periodicamente ao Congresso e à PCLOB, designadamente sobre o número e a natureza das queixas recebidas pelo departamento/organismo, bem como um resumo de tais queixas, as análises efetuadas e as questões colocadas e o impacto das atividades levadas a cabo pelo agente[107]. Segundo a avaliação das autoridades nacionais de proteção dos dados, o controlo interno exercido pelos agentes responsáveis pela proteção da privacidade e das liberdades cívicas pode ser considerado «bastante sólido», mesmo que na sua opinião esses agentes não beneficiem do grau de independência exigido[108].

97) Além disso, cada elemento do setor das informações dispõe do seu próprio *inspetor-geral* que, entre outras funções, é responsável pela supervisão das atividades de informações externas[109]. Isto inclui, no âmbito do ODNI, um *Office of the Inspector General* (gabinete do inspetor-geral) com competência abrangente sobre todo o setor das informações e autorizado a investigar queixas ou informações respeitantes a alegações de conduta ilegal ou abuso de autoridade relacionadas com o ODNI e/ou programas e atividades do setor das informações[110]. Os inspetores-gerais são unidades juridicamente independentes[111] responsáveis pela realização de auditorias e investigações relacionadas com os programas e operações levados a cabo pelo respetivo serviço para efeitos de segurança nacional, nomeadamente por abuso ou violação da lei[112]. Estão autorizados a aceder a todos os registos, relatórios, auditorias, revisões, documentos, recomendações ou outros materiais relevantes, através de intimações, se necessário, e podem recolher depoimentos[113]. Embora os inspetores-gerais apenas possam emitir recomendações não vinculativas sobre medidas corretivas, os seus relatórios, nomeadamente sobre ações de acompanhamento (ou a

---

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

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

108 Parecer 1/2016 do grupo de trabalho do artigo 29.º sobre a proteção de dados, sobre o projeto de decisão de adequação sobre o Escudo de Proteção da Privacidade UE-EUA (adotado em 13.4.2016), p. 41.

109 Declarações do ODNI (anexo VI), p. 7. Ver, por exemplo, NSA, PPD-28 Secção 4 Procedimentos, 12.1.2015, Sec. 8.1(c); CIA, *Signals Intelligence Activities, p. 7 (Responsibilities)*.

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

111 O cargo destes inspetores-gerais é assegurado e só podem ser destituídos pelo Presidente, que deve comunicar ao Congresso, por escrito, os motivos da destituição. Tal não significa necessariamente que estão completamente isentos de instruções. Em alguns casos, o chefe do departamento pode proibir o inspetor-geral de iniciar, realizar ou concluir uma auditoria ou investigação em que tal seja considerado necessário para preservar interesses nacionais importantes (em matéria de segurança). Contudo, o Congresso deve ser informado do exercício desta autoridade e, com base no que precede, poderia responsabilizar o respetivo diretor. Ver, por exemplo, *Inspector General Act* de 1978, § 8 (IG do *Department of Defense*); § 8E (IGdo DOJ), § 8G (d)(2)(A),(B) (IG da NSA); 50. U.S.C. § 403q (b) (IG da CIA); *Intelligence Authorization Act For Fiscal Year 2010*, Sec. 405(f) (IG do setor das informações). Segundo a avaliação das autoridades nacionais de proteção dos dados, os inspetores-gerais «satisfarão provavelmente o critério relativo à independência organizacional tal como definida pelo TJUE e pelo Tribunal Europeu dos Direitos do Homem (TEDH), pelo menos a partir do momento em que o novo processo de nomeação seja aplicável a todos.» Veo o Parecer 1/2016 do grupo de trabalho do artigo 29.º sobre a proteção de dados, sobre o projeto de decisão de adequação sobre o Escudo de Proteção da Privacidade UE-EUA (adotado em 13.4.2016), p. 40.

112 Ver declarações do ODNI (anexo VI), p. 7. Ver também *Inspector General Act* de 1978, com as alterações que lhe foram introduzidas, Pub. L. 113-126 de 7.7.2014.

113 Ver *Inspector General Act* de 1978, § 6.

sua inexistência) são publicados e, além disso, transmitidos ao Congresso que pode, com base neles, exercer a sua função de supervisão[114].

98) Além disso, são atribuídas à *Privacy and Civil Liberties Oversight Board*, um órgão independente[115] dentro do poder executivo constituído por um conselho bipartidário de cinco membros[116] nomeados pelo Presidente para um mandato de seis anos e aprovados pelo Senado, responsabilidades no domínio das políticas de luta contra o terrorismo e da respetiva aplicação, com vista à proteção da privacidade e das liberdades cívicas. No quadro da sua análise da ação do setor das informações, pode aceder a todos os registos, relatórios, auditorias, análises, documentos e recomendações dos serviços de informações, nomeadamente informações classificadas, realizar entrevistas e recolher depoimentos. Recebe relatórios dos agentes responsáveis pela proteção da privacidade e das liberdades cívicas de vários departamentos/serviços federais[117], pode emitir recomendações e comunica regularmente aos comités do Congresso e ao Presidente[118]. A PCLOB é igualmente responsável, dentro dos limites do seu mandato, pela preparação de um relatório de avaliação da aplicação da PPD-28.

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

100) Para facilitar a supervisão, os elementos do setor das informações são incentivados a conceber sistemas de informações que permitam o controlo, o registo e a análise das consultas ou outras pesquisas de informações pessoais[119]. Os organismos de supervisão e conformidade verificarão periodicamente as práticas dos elementos do setor das informações para proteger as informações pessoais constantes da informação de origem eletromagnética e a sua conformidade com estes procedimentos[120].

101) Além disso, estas funções de supervisão são apoiadas por amplos requisitos de comunicação no que diz respeito ao incumprimento. Em especial, os procedimentos dos serviços devem garantir que, sempre que se verifique um problema de conformidade grave que implique as informações pessoais de qualquer pessoa, independentemente da sua nacionalidade, recolhidas através de informação de origem

---

114 Ver declarações do ODNI (anexo VI), p. 7. Ver também *Inspector General Act* de 1978, §§ 4(5), 5. De acordo com a secção 405(b)(3),(4) da *Intelligence Authorization Act For Fiscal Year 2010*, Pub. L. 111-259 de 7.10.2010, o inspetor-geral do setor das informações manterá o DNI e o Congresso informados da necessidade e do progresso das medidas corretivas.

115 Segundo a avaliação das autoridades nacionais de proteção dos dados, a PCLOB demonstrou no passado «os seus poderes independentes». Ver o Parecer 1/2016 do grupo de trabalho do artigo 29.º sobre a proteção de dados, sobre o projeto de decisão de adequação sobre o Escudo de Proteção da Privacidade UE-EUA (adotado em 13.4.2016), p. 42.

116 Além disso, a PCLOB emprega cerca de 20 funcionários regulares. Ver https://www.pclob.gov/about-us/staff.html.

117 Estes incluem, pelo menos, o *Department of Justice*, o *Department of Defense*, o *Department of Homeland Security*, o *Director of National Intelligence* e a *Central Intelligence Agency*, para além de qualquer outro departamento, serviço ou elemento do poder executivo que seja designado pela PCLOB por ser adequado para efeitos de abrangência.

118 Ver 42 U.S.C. § 2000ee. Ver também o mecanismo de mediação (anexo III), secção 6, alínea b), subalínea ii). Entre outras coisas, a PCLOB deverá informar quando uma agência do poder executivo se recusar a seguir o seu conselho.

119 ODNI, *Safeguarding the Personal Information of all People: A Status Report on the Development and Implementation of Procedures under Presidential Policy Directive 28*, pp. 7-8.

120 Id. p. 8. Ver também declarações do ODNI (anexo VI), p. 9.

eletromagnética, esse problema deve ser imediatamente comunicado ao chefe do elemento do setor das informações que, nos termos da PPD-28, deve determinar se são necessárias medidas corretivas[121]. Além disso, de acordo com o Decreto Executivo n.º 12333, todos os elementos do setor das informações são obrigados a comunicar as situações de incumprimento à *Intelligence Oversight Board*[122]. Estes mecanismos asseguram que o problema será resolvido no nível mais elevado do setor das informações. Sempre que diga respeito a um cidadão de um país terceiro, o *Director of National Intelligence*, em consulta com o Secretary of State e o chefe do departamento ou serviço que efetua a notificação, deve determinar se devem ser tomadas medidas para notificar o governo estrangeiro em questão, em consonância com a proteção das fontes, dos métodos e dos funcionários dos EUA[123].

102) Em segundo lugar, para além destes mecanismos de supervisão no poder executivo, o Congresso dos EUA, especificamente os *House and Senate Intelligence and Judiciary Committees*, tem responsabilidades de supervisão no que se refere a todas as atividades de informações externas dos EUA, designadamente a informação de origem eletromagnética. De acordo com a *National Security Act* (lei relativa à segurança nacional), «[o] Presidente deve garantir que os comités de informações do Congresso são mantidos plenamente informados e atualizados sobre as atividades de informações dos Estados Unidos, nomeadamente sobre qualquer atividade de informação prevista significativa, tal como exigido pelo presente subcapítulo».[124] Além disso, «[o] Presidente deve assegurar que todas as atividades de informações ilegais são imediatamente comunicadas aos comités de informações do Congresso, a par de todas as medidas corretivas tomadas ou previstas em relação a tal atividade ilegal».[125] Os membros destes comités têm acesso a informações classificadas, bem como a métodos e programas de informações[126].

103) Legislação posterior alargou e aperfeiçoou os requisitos de comunicação, tanto relativamente aos elementos do setor das informações, como aos inspetores-gerais e ao *Attorney General*. Por exemplo, a FISA exige que o *Attorney General* «informe na íntegra» o Senado e os *House Intelligence and Judiciary Committees* relativamente às atividades do governo nos termos de determinadas secções da FISA[127]. Exige ainda que o governo apresente aos comités do Congresso cópias de «todas as decisões, decretos ou pareceres do *Foreign Intelligence Surveillance Court* ou do *Foreign Intelligence Surveillance Court of Review* que incluam construção ou interpretação significativas» das disposições da FISA. Nomeadamente, no que se refere à vigilância nos termos da secção 702 da FISA, a supervisão é exercida através de relatórios exigidos por lei apresentados aos *Intelligence and Judiciary Committees*, bem como de esclarecimentos e audições frequentes. Estes incluem um relatório semestral apresentado pelo *Attorney General* que descreve a utilização da secção 702 da FISA, com documentos de apoio que incluem, nomeadamente os relatórios de conformidade

---

121 ODNI, S*afeguarding the Personal Information of all People: A Status Report on the Development and Implementation of Procedures under Presidential Policy Directive 28*, p. 7. Ver, por exemplo, NSA, PPD-28 Secção 4 Procedimentos, 12.01.2015, Sec. 7.3, 8.7(c),(d); FBI, *Presidential Policy Directive 28 Policies and Procedures*, Sec. III (A)(4), (B)(4); CIA, *Signals Intelligence Activities*, p. 6 (*Compliance*) e p. 8 (*Responsibilities*).

122 Ver E.O. 12333, secção 1.6(c).

123 PPD-28, secção 4(a)(iv).

124 Ver Sec. 501(a)(1) (50 U.S.C. § 413(a)(1)). Esta disposição contém os requisitos gerais no que se refere à supervisão efetuada pelo Congresso no domínio da segurança nacional.

125 Ver Sec. 501(b) (50 U.S.C. § 413(b)).

126 Ver Sec. 501(d) (50 U.S.C. § 413(d)).

127 Ver 50 U.S.C. §§ 1808, 1846, 1862, 1871, 1881f.

do *Department of Justice* e do ODNI, bem como uma descrição de todas as situações de incumprimento,[128] e uma avaliação semestral distinta efetuada pelo *Attorney General* e o DNI que documenta a conformidade com os procedimentos de orientação e minimização que visam garantir que a recolha é efetuada para atingir um objetivo válido em termos de informações externas[129]. O Congresso também recebe relatórios elaborados pelos inspetores-gerais que estão autorizados a avaliar a conformidade dos serviços com os procedimentos de orientação e minimização, bem como com as orientações do *Attorney General*.

104) De acordo com a *Freedom Act* de 2015, o governo dos EUA deve divulgar anualmente ao Congresso (e ao público) o número de decisões e diretivas solicitadas e recebidas ao abrigo da FISA, bem como as estimativas do número de cidadãos norte-americanos e de países terceiros que são alvo de vigilância, entre outros[130]. 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)[131].

105) Em terceiro lugar, as atividades de informações levadas a cabo pelas autoridades públicas dos EUA com base na FISA permitem a reapreciação, e, em alguns casos, a autorização prévia das medidas pelo *Tribunal da FISA* (FISC)[132], um tribunal independente[133] cujas decisões podem ser impugnadas perante o *Foreign Intelligence Court of Review* (FISCR)[134] e, em última instância, o Supremo Tribunal dos Estados Unidos[135]. Em caso de autorização prévia, as autoridades requerentes (FBI, NSA, CIA, etc.) terão de apresentar um projeto de pedido aos advogados do *National Security*

---

128 Ver 50 U.S.C. § 1881f.

129 Ver 50 U.S.C. § 1881a(l)(1).

130 Ver *USA Freedom Act* de 2015, Pub. L. N.º 114-23, Sec. 602(a). Além disso, segundo a secção 402, «o *Director of National Intelligence*, em consulta com o *Attorney General*, deve realizar uma reapreciação de desclassificação de cada decisão ou parecer emitido pelo *Foreign Intelligence Surveillance Court* ou o *Foreign Intelligence Surveillance Court of Review* (tribunal encarregado de apreciar os recursos relativos aos pedidos e mandatos em matéria de vigilância — tal como definido na secção 601(e)) que inclua uma construção ou interpretação significativa de qualquer disposição da legislação, incluindo qualquer interpretação ou construção nova ou significativa da expressão «termo de seleção específico» e, em consonância com essa reapreciação, disponibilizar ao público, tanto quanto possível, cada um destes pareceres ou decisões».

131 *USA Freedom Act*, Sec. 602(a), 603(a).

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

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

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

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

Department do *Department of Justice* que analisarão e, se necessário, solicitarão informações adicionais[136]. Após a finalização do pedido, este terá de ser aprovado pelo *Attorney General*, *Deputy Attorney General* ou pelo *Assistant Attorney General for National Security*[137]. Subsequentemente, o *Department of Justice* apresentará o pedido ao FISC, que avaliará o pedido e emitirá uma determinação preliminar sobre a forma de proceder[138]. Sempre que ocorra uma audição, o FISC tem autoridade para recolher depoimentos que podem incluir pareceres de peritos[139].

106) O FISC (e o FISCR) são apoiados por um grupo permanente de cinco peritos em questões de segurança nacional, bem como em liberdades cívicas[140]. A partir deste grupo, o tribunal deve nomear uma pessoa para intervir na qualidade de *amicus curiae*, a fim de assistir na análise de qualquer pedido de decisão ou reapreciação que, na opinião do tribunal, apresente uma interpretação nova ou significativa do direito, a menos que o tribunal considere que tal nomeação não é adequada[141]. Em especial, tal deve garantir que as considerações em matéria de proteção da privacidade são tidas em devida conta na avaliação do tribunal. O tribunal também pode nomear uma pessoa ou organização para intervir na qualidade de *amicus curiae*, fornecendo, nomeadamente, competências técnicas, sempre que considere necessário ou, mediante pedido, autorizar uma pessoa ou organização a apresentar informações a título de *amicus curiae*[142].

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

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

---

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

137 50 U.S.C. §§ 1804 (a), 1801 (g).

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

139 PCLOB, Sec. 215 Report, p.179, n.º 619.

140 50 U.S.C. § 1803 (i)(1),(3)(A). Esta nova legislação implementou recomendações apresentadas pela PCLOB com vista a criar um grupo de peritos em questões de proteção da privacidade e das liberdades cívicas que possa intervir na qualidade de *amicus curiae*, a fim de fornecer ao tribunal os argumentos jurídicos conducentes ao aumento da proteção da privacidade e das liberdades cívicas. Ver PCLOB, Sec. 215 Report, pp. 183-187.

141 50 U.S.C. § 1803 (i)(2)(A). De acordo com as informações apresentadas pelo ODNI, tais nomeações já ocorreram. Ver *Signals Intelligence Reform, 2016 Progress Report.*

142 50 U.S.C. § 1803 (i)(2)(B).

143 50 U.S.C. § 1861

enumeração dos procedimentos de minimização adotados pelo *Attorney General* para a preservação e divulgação das informações recolhidas. [144]

109) Pelo contrário, nos termos da secção 702 da FISA[145], o FISC não autoriza medidas de vigilância individuais; em vez disso, autoriza programas de vigilância (tais como o PRISM e o UPSTREAM) com base em certificações anuais elaboradas pelo *Attorney General* e o *Director of National Intelligence*. A secção 702 da FISA permite que se visem pessoas que se acredite estarem localizadas fora dos Estados Unidos a fim de obter informações no estrangeiro[146]. Esta seleção da pessoa visada é realizada pela NSA em duas fases: em primeiro lugar, os analistas da NSA identificaram os cidadãos de países terceiros localizados no estrangeiro cuja vigilância conduzirá, com base na avaliação do analista, às informações externas relevantes especificadas na certificação. Em segundo lugar, após a identificação destas pessoas e a sua aprovação como objetivos por um amplo mecanismo de análise no âmbito da NSA[147], 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[148]. Tal como indicado, as certificações a aprovar pelo FISC não contêm informações sobre as pessoas visadas, mas sim categorias de identificação das informações no estrangeiro[149]. Embora o FISC não avalie — com base numa causa provável ou em qualquer outra norma — se as pessoas são adequadamente visadas para efeitos de obtenção de informações externas,[150] o seu controlo alarga-se à condição de que «um objetivo significativo da recolha consiste na obtenção de informações no estrangeiro»[151]. Com efeito, nos termos da secção 702 do FISA, a NSA pode recolher comunicações de cidadãos de países terceiros fora dos EUA apenas se for possível considerar razoavelmente que um determinado meio de comunicação está a ser utilizado para comunicar informações no estrangeiro (por exemplo, relacionadas com terrorismo internacional, proliferação nuclear ou atividades cibernéticas hostis). As determinações para este efeito são objeto de controlo jurisdicional[152]. As certificações também necessitam de prever procedimentos de orientação e minimização[153]. O *Attorney General* e o *Director of National Intelligence* verificam a conformidade e os serviços são obrigados a comunicar todas as situações de incumprimento ao FISC[154] (bem como ao Congresso e à *Intelligence*

144 50 U.S.C. § 1861 (b).
145 50 U.S.C. § 1881.
146 50 U.S.C. § 1881a (a).
147 PCLOB, Sec. 702 *Report*, p. 46.
148 50 U.S.C. § 1881a (h).
149 50 U.S.C. § 1881a (g). De acordo com a PCLOB, até à data, estas categorias dizem respeito sobretudo ao terrorismo internacional e a temas como a aquisição de armas de destruição maciça. Ver PCLOB, Sec. 702 *Report*, p. 25.
150 PCLOB, Sec. 702 *Report*, p. 27.
151 50 U.S.C. § 1881a.
152 «*Liberty and Security in a Changing World*», *Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies*, 12.12.2013, p. 152.
153 50 U.S.C.1881a (i).
154 A regra 13, alínea b), do regulamento interno do FISC exige que o governo informe o Tribunal, por escrito, imediatamente após a descoberta de que uma autorização ou aprovação concedida pelo Tribunal foi implementada de forma contrária à autorização ou aprovação do Tribunal, ou à legislação aplicável. Exige ainda que o governo notifique o tribunal por escrito dos factos e circunstâncias relevantes para tal incumprimento. Normalmente, o governo apresentará uma notificação final relativa à regra 13, alínea a), depois de tomar conhecimento dos factos relevantes e da destruição de todas as informações decorrentes da recolha não autorizada. Ver *Walton Letter*, p. 10.

Oversight Board do Presidente), que, com base no que precede, pode alterar a autorização[155].

110) Além disso, a fim de aumentar a eficiência da supervisão pelo FISC, a administração dos EUA concordou em implementar uma recomendação apresentada pela PCLOB com o objetivo de fornecer ao FISC documentação relativa às decisões sobre a seleção de alvos nos termos da secção 702, designadamente uma amostra aleatória de formulários de atribuição de missões, para permitir ao FISC avaliar de que modo o requisito para efeitos de informações externas é cumprido na prática[156]. Ao mesmo tempo, a administração dos EUA aceitou e tomou medidas para rever os procedimentos de seleção de alvos da NSA para documentar melhor os motivos para a recolha de informações externas apresentados nas decisões relativas à seleção de alvos[157].

Reparação individual

111) Existem várias vias acessíveis nos termos da legislação dos EUA aos titulares de dados da UE caso estes tenham preocupações relativamente à possibilidade de os seus dados pessoais terem sido tratados (recolhidos, avaliados, etc.) por elementos do setor das informações dos EUA, e em caso positivo, se as limitações aplicáveis na legislação dos EUA foram cumpridas. Essencialmente estas dizem respeito a três domínios: ingerência nos termos da FISA; acesso ilegal e intencional aos dados pessoais por parte de funcionários do governo; e acesso à informação nos termos da *Freedom of Information Act* (lei relativa à liberdade de informação — FOIA)[158].

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

---

155 50 U.S.C. § 1881 (l). Ver também PCLOB, Sec. 702 Report, pp. 66-76; *NSA CLPO, NSA's Implementation of Foreign Intelligence Surveillance Act Section 702*, 16.4.2014. A recolha de dados pessoais para efeitos de informações nos termos da secção 702 da FISA é objeto de supervisão interna e externa no seio do poder executivo. Entre outros, a supervisão interna inclui programas de conformidade interna para avaliar e supervisionar a conformidade com os procedimentos de orientação e minimização; comunicação de situações de incumprimento, tanto a nível interno como externo ao ODNI, ao *Department of Justice*, ao Congresso e ao FISC; e reapreciações anuais transmitidas aos mesmos organismos. No que se refere à supervisão externa, esta é constituída sobretudo por análises de orientação e minimização realizadas pelo ODNI, o DOJ, e os inspetores-gerais, que, por sua vez, comunicam ao Congresso e a FISC, designadamente sobre situações de incumprimento. As situações de incumprimento graves devem ser imediatamente comunicadas ao FISC e as restantes devem ser comunicadas num relatório trimestral. Ver PCLOB, Sec. 702 *Report*, pp. 66-77.

156 PCLOB, *Recommendations Assessment Report*, 29.1.2015, p. 20.

157 PCLOB, *Recommendations Assessment Report*, 29.1.2015, p. 16.

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

159 Ver as seguintes declarações do ODNI (anexo VI), p. 16.

160 18 U.S.C. § 2712.

161 50 U.S.C. § 1810.

caso o governo dos EUA tencione utilizar ou divulgar quaisquer informações obtidas ou decorrentes de vigilância eletrónica contra a pessoa em processos judiciais ou administrativos nos Estados Unidos[162].

113) Em segundo lugar, o governo dos EUA remeteu a Comissão para várias vias de recurso adicionais que os titulares de dados da UE podem utilizar para efeitos de recurso contra funcionários do governo em virtude do acesso, ou da utilização, ilegal por parte do governo, de dados pessoais, nomeadamente para alegados efeitos de segurança nacional (isto é, a *Computer Fraud and Abuse Act*[163]; a *Electronic Communications Privacy Act*[164]; e a *Right to Financial Privacy Act*[165]). Todas estas ações são referentes a dados, alvos e/ou tipos de acesso específicos (por exemplo, acesso remoto a um computador através da Internet) e encontram-se disponíveis em determinadas condições (por exemplo, conduta intencional/deliberada, conduta fora da capacidade oficial, danos sofridos)[166]. Uma possibilidade mais geral de recurso está prevista na *Administrative Procedure Act* (5 U.S.C. § 702), segundo a qual «qualquer pessoa que sofra um prejuízo resultante de uma decisão de uma agência ou que é afetada ou lesada pela decisão de uma agência», pode interpor um recurso judicial. Tal inclui a possibilidade de solicitar ao tribunal «que declare ilegais e anule a atuação, os resultados e as conclusões da agência, que se venham a verificar [...] arbitrários, caprichosos, um abuso de poder, ou de outro modo não conformes ao direito»[167].

114) Por último, o governo dos EUA salientou a FOIA como um meio para os cidadãos de países terceiros solicitarem o acesso a documentação existente dos serviços federais, nomeadamente nos casos em que esta contenha os dados pessoais do respetivo titular[168]. Devido à sua incidência, a FOIA não prevê uma via de recurso individual contra a ingerência nos dados pessoais como tal, embora possa, em princípio, permitir que as pessoas obtenham acesso a informações relevantes conservadas por serviços de informações nacionais. Mesmo a este respeito, as possibilidades parecem ser limitadas, uma vez que os serviços podem reter informações abrangidas por determinadas exceções enumeradas, nomeadamente o acesso a informações de segurança nacional classificadas e informações relativas a investigações relacionadas com a aplicação da lei[169]. Tomando em consideração o que precede, a utilização de tais exceções pelos serviços de informações nacionais pode ser contestada pelas pessoas, que podem solicitar o controlo jurisdicional e administrativo.

115) Embora as pessoas, incluindo os titulares de dados da UE, disponham de várias vias de recurso se tiverem sido objeto de vigilância (eletrónica) ilegal para efeitos de segurança nacional, é igualmente evidente que pelo menos algumas bases jurídicas que os serviços de informações dos EUA podem utilizar (por exemplo E.O. 12333) não são abrangidas. Além disso, mesmo nos casos em que, em princípio, existem possibilidades de recurso judicial para cidadãos de países terceiros, como no que diz

---

162 50 U.S.C. § 1806.
163 18 U.S.C. § 1030.
164 18 U.S.C. §§ 2701-2712.
165 12 U.S.C. § 3417.
166 Declarações do ODNI (anexo VI), p. 17.
167 5 U.S.C. § 706(2)(A).
168 5 U.S.C. § 552. Existem leis semelhantes a nível estadual.
169 Caso tal se verifique, em regra, a pessoa receberá apenas uma resposta-padrão através da qual o serviço não confirma nem desmente a existência de qualquer documentação. Ver *ACLU v. CIA*, 710 F.3d 422 (D.C. Cir. 2014).

respeito à vigilância ao abrigo da FISA, as causas de ação disponíveis são limitadas[170] e as ações apresentadas por pessoas singulares (incluindo cidadãos dos EUA) serão declaradas inadmissíveis se não conseguirem demonstrar «legitimidade»[171], o que limita o acesso aos tribunais comuns[172].

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

117) Em especial, de acordo com os compromissos do governo dos EUA, o mecanismo de mediação assegurará que as queixas individuais são investigadas e abordadas de forma adequada e que as pessoas recebem uma confirmação independente de que as leis dos EUA foram cumpridas ou, no caso de uma violação dessas leis, que o incumprimento foi corrigido[173]. O mecanismo inclui «o Mediador para o Escudo de Proteção da Privacidade», ou seja, o *Under-Secretary* e outro pessoal, assim como outros órgãos de supervisão competentes para controlar os diversos elementos dos serviços de informação em cuja cooperação o Mediador para o Escudo de Proteção da Privacidade se baseará para tratar das queixas. Em especial, quando o pedido de uma pessoa se refira à compatibilidade da vigilância com a legislação americana, o Mediador para o Escudo de Proteção da Privacidade poderá confiar em organismos de supervisão independentes com competências de investigação (como os inspetores-gerais e a PCLOB). Em cada caso, o *Secretary of State* garantirá que o Mediador disporá dos meios para assegurar que a sua resposta aos pedidos individuais se baseie em todas as informações necessárias.

118) Através desta «estrutura composta», o mecanismo de mediação garante uma supervisão independente e um recurso individual. Além disso, a cooperação com outros organismos de supervisão assegura o acesso aos conhecimentos especializados necessários. Por último, ao impor ao Mediador para o Escudo de Proteção da Privacidade a obrigação de confirmar o cumprimento ou a correção de um

---

[170] Ver declarações do ODNI (anexo VI), p. 16. De acordo com as explicações apresentadas, as causas de ação disponíveis exigem a existência de *danos* (18 U.S.C. § 2712; 50 U.S.C. § 1810) ou uma demonstração de que o *governo pretende utilizar ou divulgar informações* obtidas ou decorrentes de vigilância eletrónica do titular dos dados contra essa pessoa *em processos judiciais ou administrativos* nos Estados Unidos (50 U.S.C. § 1806). Contudo, tal como o Tribunal de Justiça salientou repetidamente, para determinar a existência de uma ingerência no direito fundamental à privacidade, é indiferente se o titular dos dados sofreu consequências adversas em virtude dessa ingerência. Ver *Schrems*, n.º 89 com referências adicionais.

[171] Este critério de admissibilidade advém do requisito de «caso ou controvérsia» da Constituição dos EUA, artigo III.

[172] Ver *Clapper v. Amnesty Int'l USA*, 133 S.Ct. 1138, 1144 (2013). No que se refere à utilização de NSL, a *Freedom Act* (secção 502(f)-503) prevê que os requisitos de não divulgação devem ser periodicamente reexaminados e que os *destinatários* de NSL devem ser notificados sempre que os factos deixem de apoiar um requisito de não notificação (ver declarações do ODNI (anexo VI), p. 13). Contudo, tal não garante que o titular de dados da UE seria informado de que foi objeto de uma investigação.

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

incumprimento, o mecanismo reflete um compromisso do governo dos EUA no seu conjunto de tratar e resolver as queixas apresentadas por cidadãos da UE.

119) Em primeiro lugar, ao contrário de um mecanismo exclusivamente intragovernamental, o Mediador para o Escudo de Proteção da Privacidade receberá e responderá a queixas individuais. Tais queixas podem ser dirigidas às autoridades de supervisão dos Estados-Membros competentes em matéria de supervisão dos serviços de segurança nacional e/ou do tratamento dos dados pessoais pelas autoridades públicas, que as apresentarão a um organismo centralizado a nível da UE, que as enviará ao Mediador para o Escudo de Proteção da Privacidade[174]. Com efeito, tal beneficiará os cidadãos da UE, que podem recorrer a uma autoridade nacional «perto de casa» e na própria língua. A função de tal autoridade consistirá em apoiar o cidadão na apresentação de um pedido junto do Mediador para o Escudo de Proteção da Privacidade que contém as informações de base podendo, assim, ser considerado «completo». A pessoa não tem de demonstrar que o governo dos EUA acedeu, de facto, aos seus dados pessoais através de atividades de informação de origem eletromagnética.

120) Em segundo lugar, o governo americano compromete-se a garantir que, no exercício das suas funções, o Mediador para o Escudo de Proteção da Privacidade poderá apoiar-se na cooperação de outros mecanismos de verificação do cumprimento e de supervisão previstos no direito dos EUA. Tal implicará por vezes os serviços de informações nacionais, em especial se o pedido tiver de ser interpretado como um pedido de acesso a documentos relacionados com a *Freedom of Information Act*. Noutros casos, em especial quando os pedidos dizem respeito à compatibilidade da vigilância com a legislação dos EUA, tal cooperação implicará organismos de supervisão independentes (por exemplo, inspetores-gerais) com a responsabilidade e poder para realizar uma investigação aprofundada (em especial através do acesso a todos os documentos pertinentes e competência para solicitar informações e declarações) e abordar casos de incumprimento[175]. Além disso, o Mediador para o Escudo de Proteção da Privacidade terá a capacidade de submeter questões à PCLOB para análise[176]. Nos casos em que um destes organismos de supervisão tenha detetado qualquer incumprimento, os serviços de informação em questão (por exemplo, uma agência de informações) terá de corrigir o incumprimento, uma vez que apenas deste modo o Mediador poderá garantir uma resposta «positiva» à pessoa (ou seja, que se corrigiu o incumprimento), em relação ao qual o governo americano se comprometeu. Por outro lado, no quadro da cooperação, o Mediador para o Escudo de Proteção da Privacidade será informado dos resultados da investigação, e disporá dos meios para garantir que recebe todas as informações necessárias para preparar a resposta.

---

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

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

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

121) Por último, o Mediador para o Escudo de Proteção da Privacidade será um órgão independente e, como tal, não receberá instruções dos serviços de informações dos EUA[177]. O que precede é especialmente importante, uma vez que o mediados terá de «confirmar» que i) a queixa foi devidamente investigada e que ii) a legislação dos EUA pertinente — nomeadamente as limitações e garantias estabelecidas no anexo VI — foi cumprida ou, em caso de incumprimento, que tal infração foi corrigida. A fim de poder fornecer esta confirmação independente, o Mediador para o Escudo de Proteção da Privacidade terá de receber as informações necessárias relativamente à investigação para avaliar a exatidão da resposta à queixa. Além disso, o *Secretary of State* comprometeu-se a garantir que o *Under-Secretary* desempenhará as funções de Mediador para o Escudo de Proteção da Privacidade de froma objetiva e sem quaisquer influências indevidas suscetíveis de terem um efeito na resposta a dar.

122) Globalmente, este mecanismo assegura que as queixas individuais serão investigadas de forma aprofundada e tratadas, e que, pelo menos no domínio da vigilância, se recorra a organismos de supervisão independentes com as competências e os poderes de investigação necessários e um Mediador que possa exercer as suas funções sem quaisquer influências indevidas, especialmente a nível político. Além disso, as pessoas poderão apresentar queixas sem terem de demonstrar, ou mesmo fornecer elementos que indiquem que foram objeto de vigilância[178]. Tendo em conta estes elementos, a Comissão congratula-se por ver que existem garantias adaptadas e eficazes contra os abusos.

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

124) Relativamente a este aspeto, a Comissão toma nota do acórdão do Tribunal de Justiça proferido no processo *Schrems*, segundo o qual «uma regulamentação que não preveja nenhuma possibilidade de o particular recorrer a vias de direito para ter acesso aos dados pessoais que lhe dizem respeito, ou para obter a retificação ou a supressão de tais dados, não respeita o conteúdo essencial do direito fundamental a uma proteção jurisdicional efetiva, tal como é consagrado no artigo 47.° da Carta.»[179] A avaliação da Comissão confirmou que tais vias de recurso estão previstas nos Estados Unidos, em especial através da introdução da figura do Mediador. Esta figura dispõe de poderes de supervisão independente com competências de investigação. No quadro da sua supervisão contínua do Escudo de Proteção da Privacidade, nomeadamente através da análise conjunta anual em que também participará o Mediador, a Comissão reapreciará a eficácia deste mecanismo.

---

177 Ver *Roman Zakharov/Rússia*, Acórdão de 4.12.2015 (Grande Secção), Queixa n.º 47143/06, n.º 275 (embora seja em princípio desejável que a função de supervisão seja confiada a um juiz, podendo a supervisão efetuada por um órgão não judicial ser considerada compatível com a Convenção, desde que esse órgão de supervisão seja independente das autoridades que procedem à supervisão e seja investida de poderes e atribuições suficientes).

178 Ver *Kennedy/Reino Unido*, Acórdão de 18.5.2010, Queixa n.º 26839/05, n.º 167.

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

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

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

126) De acordo com estas informações, nos termos da Quarta Emenda da Constituição dos EUA[180], as buscas e apreensões efetuadas pelas autoridades com funções coercivas[181] exigem principalmente um mandado judicial após a demonstração de uma «causa provável». Nos poucos casos excecionais e especificamente estabelecidos nos quais o requisito de um mandado não é aplicável[182], o exercício das funções coercivas é objeto de um teste de «razoabilidade»[183]. Determina-se se uma busca ou apreensão é razoável «através da avaliação, por um lado, da medida em que invade a privacidade de uma pessoa e, por outro lado, da medida em que é necessária para a promoção de interesses governamentais legítimos».[184] Em termos mais gerais, a Quarta Emenda garante a privacidade, a dignidade e assegura a proteção contra atos arbitrários e invasivos por parte de funcionários do governo[185]. Estes conceitos refletem a ideia de necessidade e proporcionalidade constante do direito da União. Quando as autoridades com funções coercivas já não precisam de utilizar os elementos apreendidos como provas, devem restituí-los[186].

127) Embora o direito decorrente da Quarta Emenda não abranja os cidadãos de países terceiros não residentes nos Estados Unidos, estes últimos beneficiam, indiretamente da sua proteção, dado que são as empresas dos EUA que detêm dados pessoais, devendo as autoridades com funções coercivas em qualquer caso obter autorização judicial (ou pelo menos respeitar o requisito de razoabilidade[187]. Outras salvaguardas

---

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

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

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

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

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

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

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

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

decorrem de competências jurídicas especiais, bem como das orientações do *Department of Justice*, que limitam o acesso aos dados das autoridades com funções coercivas por motivos equivalentes à necessidade e proporcionalidade (por exemplo, exigindo que o FBI utilize os métodos de investigação menos invasivos possíveis, tomando em consideração o efeito sobre a privacidade e as liberdades cívicas)[188]. Segundo as declarações apresentadas pelo governo dos EUA, são aplicáveis proteções idênticas ou mais elevadas às investigações das autoridades com funções coercivas a nível estadual (no que se refere às investigações executadas ao abrigo das leis estaduais)[189].

128) Embora uma autorização judicial prévia concedida por um tribunal ou júri (um braço de investigação do tribunal reunido por um juiz ou magistrado) não seja necessária em todos os casos[190], as intimações administrativas estão limitadas a casos específicos e serão objeto de um controlo jurisdicional independente pelo menos nos casos em que o governo solicite uma execução em tribunal[191].

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

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

131) Em geral, ao abrigo das disposições relativas a um recurso judicial da *Administrative Procedure Act*, [192] «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[193]. Tal inclui a possibilidade de solicitar ao tribunal «que declare ilegais e anule a atuação, os resultados e as conclusões da agência, que se

188 Declarações do DOJ (anexo VII), p. 4 com referências adicionais.

189 Declarações do DOJ (anexo VII), n.º 2.

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

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

192 5 U.S.C. § 702.

193 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.

venham a verificar [...] arbitrários, caprichosos, um abuso de poder, ou de outro modo não conformes ao direito»[194].

132) Mais especificamente, o título II da *Electronic Communications Privacy Act*[195] 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[196]. Criminaliza o acesso ilegal (ou seja, não autorizado pelo tribunal ou admissível de outro modo) a essas comunicações e prevê que uma pessoa afetada possa intentar uma ação cível num tribunal federal dos EUA para obter reparação por danos efetivos e punitivos, bem como uma compensação equitativa contra um funcionário do governo que tenha cometido intencionalmente esses atos ilegais, ou contra os Estados Unidos.

133) Do mesmo modo, ao abrigo da *Freedom of Information Act* (FOIA, 5 U.S.C. § 552), qualquer pessoa tem o direito de obter acesso aos registos de uma agência federal e, após o esgotamento das soluções administrativas, de fazer valer esse direito em tribunal, exceto na medida em que esses registos sejam protegidos de divulgação pública por uma isenção ou uma exclusão especial decorrente do exercício de funções coercivas[197].

134) Além disso, várias outras leis garantem às pessoas o direito de intentar um processo contra uma autoridade pública ou um funcionário americano no que diz respeito ao tratamento dos seus dados pessoais, tais como a *Wiretap Act*[198], a *Computer Fraud*

---

194 5 U.S.C. § 706(2)(A).

195 18 U.S.C. §§ 2701-2712.

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

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

198 18 U.S.C. §§ 2510 e seg. Ao abrigo da *Wiretap Act* (18 U.S.C. § 2520), uma pessoa cuja comunicação telefónica, verbal ou eletrónica é intercetada, divulgada ou deliberadamente utilizada pode intentar uma ação cível por violação da *Wiretap Act*, incluindo, em certas circunstâncias, contra um funcionário do governo ou contra os Estados Unidos. Para a recolha de informações relativas ao endereço e outras informações não referentes ao conteúdo (por exemplo, endereço IP, endereço eletrónico destinatário/emissor), ver igualmente

and Abuse Act[199], a *Federal Torts Claim Act*[200], a *Right to Financial Privacy Act*[201], e a *Fair Credit Reporting Act*[202].

135) Por conseguinte, a Comissão conclui que existem normas em vigor nos Estados Unidos destinadas a limitar qualquer ingerência, para efeitos do exercício de funções coercivas[203] ou outros efeitos de interesse público, nos direitos fundamentais das pessoas cujos dados pessoais são transferidos da União para os Estados Unidos ao abrigo do Escudo de Proteção da Privacidade UE-EUA ao estritamente necessário para a consecução do objetivo legítimo em questão e que asseguram a proteção jurídica eficaz contra tal ingerência.

4. Nível de proteção adequado ao abrigo do Escudo de Proteção da Privacidade UE-EUA

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

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

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

139) Além disso, a Comissão considera que, como um todo, os mecanismos de supervisão e recurso previstos pelo Escudo de Proteção permitem, na prática, a identificação e

---

o capítulo «*Pen Registers and Trap and Trace Devices* do título 18 (18 U.S.C. §§ 3121-3127 e, para uma ação cível, § 2707).

199 18 U.S.C. § 1030. Ao abrigo da *Computer Fraud and Abuse Act*, qualquer pessoa pode intentar uma ação contra qualquer pessoa por acesso não autorizado intencional (ou por ter excedido um acesso autorizado) a fim de obter informações junto de um estabelecimento financeiro, de um sistema informático das autoridades americanas ou de um outro sistema específico, incluindo, em certas circunstâncias, contra um funcionário do governo.

200 28 U.S.C. §§ 2671 e seg. Ao abrigo da *Federal Tort Claims Act*, qualquer pessoa pode intentar uma ação, em certas circunstâncias, contra os Estados Unidos no que diz respeito a «atos ou omissões negligentes ou ilegítimas que comete qualquer funcionário do Estado agindo no quadro das suas funções ou do seu emprego.»

201 12 U.S.C. §§ 3401 e seg. Ao abrigo da *Right to Financial Privacy Act*, qualquer pessoa pode intentar uma ação, em certas circunstâncias, contra os Estados Unidos por obtenção ou divulgação de documentos financeiros protegidos em violação da lei. O acesso do governo aos documentos financeiros protegidos é, em geral, proibido, a menos que o governo efetue o pedido mediante uma intimação legal ou um mandato de busca ou, sujeito a limitações, um pedido escrito oficial e que a pessoa, relativamente à qual são solicitadas informações, receba notificação do pedido.

202 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.

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

sanção das infrações aos princípios de privacidade por parte das organizações aderentes ao Escudo de Proteção da Privacidade e oferecem vias de recurso ao titular de dados que lhe dão acesso aos seus dados pessoais, permitindo a retificação ou eliminação de tais dados.

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

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

5. Ação das autoridades responsáveis pela proteção dos dados e informação à Comissão

142) No acórdão *Schrems*, o Tribunal de Justiça esclareceu que a Comissão não tem competência para limitar os poderes das APD decorrentes do artigo 28.º da Diretiva 95/46/CE (nomeadamente o poder de suspensão de transferências de dados) sempre que uma pessoa, na apresentação de um pedido nos termos da referida disposição, questione a compatibilidade de uma decisão de adequação da Comissão com a proteção do direito fundamental à privacidade e à proteção dos dados[204].

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

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

[204] *Schrems*, n.os 40 e seguintes, 101-103.
[205] *Schrems*, n.os 51, 52 e 62.

de recurso que lhe permite apresentar tais objeções perante um tribunal nacional que, em caso de dúvida, deve suspender a instância e efetuar um pedido de decisão prejudicial ao Tribunal de Justiça[206].

6. Reapreciação periódica da verificação de adequação

145) Tomando em consideração o facto de o nível de proteção conferido pela ordem jurídica dos EUA poder ser suscetível de alterações, a Comissão, na sequência da adoção da presente decisão, verificará periodicamente se as conclusões relativas à adequação do nível de proteção assegurado pelos Estados Unidos ao abrigo do Escudo de Proteção da Privacidade UE-EUA se mantêm factual e legalmente justificadas. De qualquer modo, tal verificação é necessária sempre que a Comissão obtenha informações que suscitem dúvidas justificadas a esse respeito[207].

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

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

148) No âmbito da reapreciação conjunta anual, a Comissão solicitará que o *Department of Commerce* apresente informações abrangentes sobre todos os aspetos relevantes do funcionamento do Escudo de Proteção da Privacidade UE-EUA, nomeadamente queixas submetidas ao *Department of Commerce* pelas APD e os resultados das verificações de conformidade oficiosas. A Comissão também solicitará esclarecimentos relativamente a quaisquer questões ou assuntos relativos ao Escudo de Proteção da Privacidade UE-EUA e ao seu funcionamento decorrentes das informações disponíveis, nomeadamente relatórios de transparência autorizados nos termos da *Freedom Act*, relatórios públicos elaborados pelos serviços de informações nacionais dos EUA, pelas APD, grupos de proteção da privacidade, relatórios dos

[206] *Schrems*, n.º 65.
[207] *Schrems*, n.º 76.

meios de comunicação social ou outras fontes possíveis. Além disso, a fim de facilitar a tarefa da Comissão a este respeito, os Estados-Membros devem informar a Comissão dos casos em que as ações dos organismos responsáveis por assegurar a conformidade com os princípios nos EUA não asseguram essa conformidade, bem como de quaisquer indícios de que as ações das autoridades públicas dos EUA responsáveis pela segurança nacional ou pela prevenção, investigação, deteção ou repressão de infrações penais não asseguram o nível de proteção exigido.

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

7. Suspensão da decisão de adequação

150) Sempre que, com base nas verificações ou em quaisquer outras informações disponíveis, a Comissão conclua que o nível de proteção assegurado pelo Escudo de Proteção da Privacidade já não pode ser considerado como fundamentalmente equivalente ao que é garantido na União ou que existem indícios claros de que a conformidade efetiva com os princípios nos Estados Unidos pode já não estar assegurada, ou que as ações das autoridades públicas dos EUA responsáveis pela segurança nacional ou pela prevenção, investigação, deteção ou repressão de infrações penais não asseguram o nível de proteção exigido, a Comissão informará o *Department of Commerce* deste facto e solicitará a tomada de medidas adequadas a fim de resolver rapidamente os potenciais incumprimentos dos princípios num prazo especificado e razoável. Se, após o termo do prazo especificado, as autoridades dos EUA não demonstrarem de modo satisfatório que o Escudo de Proteção da Privacidade UE-EUA continua a assegurar o cumprimento efetivo e um nível de proteção adequado, a Comissão dará início a um procedimento conducente à suspensão parcial ou total ou à revogação da presente decisão[208]. Em alternativa, a Comissão pode propor a alteração da presente decisão, por exemplo, limitando o âmbito de aplicação da verificação de adequação apenas às transferências de dados sujeitas a condições adicionais.

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

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

(b) Não resolução eficaz das queixas apresentadas pelos titulares de dados da UE; a este respeito, a Comissão tomará em consideração todas as circunstâncias que afetam a possibilidade de os titulares de dados da UE fazerem valer os seus direitos, incluindo, nomeadamente, o compromisso

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

assumido voluntariamente pelas empresas autocertificadas dos EUA de cooperar com as APD e respeitar o seu aconselhamento; ou

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

152) A Comissão também ponderará dar início ao procedimento conducente à alteração, suspensão ou revogação da presente decisão se, no contexto da reapreciação conjunta anual do funcionamento do Escudo de Proteção da Privacidade UE-EUA ou de outro modo, o *Department of Commerce* ou outros departamentos ou serviços envolvidos na implementação do Escudo de Proteção da Privacidade, ou, no que se refere a questões relacionadas com segurança nacional, os representantes do setor das informações dos EUA ou o Mediador, não apresentarem as informações ou os esclarecimentos necessários para a verificação de conformidade com os princípios, da eficácia dos procedimentos para a resolução de queixas ou qualquer redução do nível de proteção exigido em consequência de ações dos serviços de informações nacionais dos EUA, designadamente na sequência da recolha e/ou do acesso a dados pessoais que não se limitem ao estritamente necessário e proporcionado. A este respeito, a Comissão tomará em consideração em que medida as informações relevantes podem ser obtidas a partir de outras fontes, nomeadamente através de relatórios de empresas autocertificadas dos EUA, conforme permitido nos termos da *Freedom Act*.

153) O grupo de trabalho relativo à proteção das pessoas no que diz respeito ao tratamento de dados pessoais criado ao abrigo do artigo 29.º da Diretiva 95/46/CE publicou o seu parecer sobre o nível de proteção assegurado pelo Escudo de Proteção da Privacidade UE-EUA[209], que foi tomado em consideração na elaboração da presente decisão.

154) O Parlamento Europeu adotou uma resolução sobre os fluxos de dados transatlânticos[210].

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

[209] Parecer 01/2016 sobre o projeto de decisão relativa ao nível de proteção assegurado pelo Escudo de Proteção da Privacidade UE-EUA, adotado em 13.4.2016.

[210] Resolução do Parlamento Europeu de 26 de maio de 2016 sobre os fluxos de dados transatlânticos ((2016/2727(RSP)).

ADOTOU A PRESENTE DECISÃO:

Artigo 1.º

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

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

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

Artigo 2.º

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

Artigo 3.º

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

Artigo 4.º

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

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

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

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

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

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

- de que as autoridades públicas dos EUA não cumprem as declarações e os compromissos constantes dos documentos que figuram em anexo à presente decisão, nomeadamente no que diz respeito às condições e limitações aplicáveis ao acesso pelas autoridades públicas dos EUA com funções coercivas, responsáveis pela segurança nacional e outros interesses públicos aos dados pessoais transferidos ao abrigo do Escudo de Proteção da Privacidade UE-EUA;
- da não resolução sistemática das queixas apresentadas pelos titulares de dados da UE; ou
- da não apresentação sistemática, por parte do Mediador para o Escudo de Proteção da Privacidade, de respostas adequadas e em tempo útil aos pedidos dos titulares de dados da UE tal como previsto no anexo III, secção 4, alínea e).

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

Artigo 5.º

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

Artigo 6.º

Os destinatários da presente decisão são os Estados-Membros.

Feito em Bruxelas, em 12.7.2016

Pela Comissão
Věra JOUROVÁ
Membro da Comissão

CÓPIA AUTENTICADA
Pelo Secretário-Geral,

Jordi AYET PUIGARNAU
Director da Secretaria
COMISSAO EUROPEIA