COMISSÃO
EUROPEIA

Bruxelas, 9.10.2024
COM(2024) 451 final

RELATÓRIO DA COMISSÃO AO PARLAMENTO EUROPEU E AO CONSELHO

sobre a primeira avaliação periódica do funcionamento da decisão de adequação relativa ao Quadro de Privacidade de Dados UE-EUA

1. PRIMEIRA AVALIAÇÃO PERIÓDICA — CONTEXTO, PREPARAÇÃO E PROCESSO

Na sua decisão de 10 de julho de 2023 («decisão de adequação»), a Comissão concluiu que o Quadro de Privacidade de Dados UE-EUA (QPD) proporciona um nível adequado de proteção dos dados pessoais transferidos da União Europeia para organizações localizadas nos Estados Unidos da América[1]. A decisão de adequação obriga a Comissão a realizar avaliações periódicas, a primeira das quais deve ter lugar um ano a contar da data de notificação da decisão de adequação aos Estados-Membros. O presente relatório conclui essa primeira avaliação.

Como exigido no considerando 211 da decisão de adequação, esta primeira avaliação, realizada após o primeiro ano de funcionamento do novo quadro, centrou-se em verificar se todos os elementos previstos no quadro foram aplicados e estão a funcionar eficazmente. A avaliação abrangeu todos os aspetos do funcionamento do quadro, nomeadamente à luz da evolução do quadro jurídico ocorrida desde a adoção da decisão de adequação.

Para preparar a avaliação, a Comissão recolheu informações das partes interessadas pertinentes, em especial de organizações não governamentais (ONG) com conhecimentos especializados em direitos digitais e privacidade[2], de organizações certificadas no âmbito do QPD, através das suas associações comerciais[3], bem como das autoridades dos EUA envolvidas na aplicação do quadro. Além disso, a Comissão também recolheu reações do público em geral através de um convite à apreciação específico no portal «Dê a sua opinião»[4].

Em 18 e 19 de julho de 2024, realizou-se uma reunião de avaliação em Washington D.C., cuja abertura ficou a cargo do membro da Comissão Europeia responsável pela Justiça e Consumidores, Didier Reynders, e pela secretária do Comércio dos EUA, Gina Raimondo[5].

---

[1] Decisão de Execução (UE) 2023/1795 da Comissão, de 10 de julho de 2023, nos termos do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho sobre a adequação do nível de proteção dos dados pessoais no âmbito Quadro de Privacidade de Dados UE-EUA.

[2] A Comissão enviou um questionário a nove ONG (Human Rights Watch, American Civil Liberties Union, Consumer Federation of America, Center for Digital Democracy, New America Open Technology Institute, Access Now, Electronic Frontier Foundation, Electronic Privacy Information Center, Center for Democracy and Technology), que incidia sobre os desenvolvimentos pertinentes no quadro jurídico dos EUA, os mecanismos de supervisão e de aplicação e o funcionamento dos mecanismos de recurso. Em 9 de julho de 2024, os serviços da Comissão e os representantes do Comité Europeu para a Proteção de Dados (CEPD) também se reuniram em linha com estas ONG.

[3] A Comissão enviou um questionário a nove associações comerciais (Software &Information Industry Association, Câmara de Comércio dos EUA, Information Technology Industry Council, Software Alliance, Centre for Information Policy Leadership, Interactive Advertising Bureau, United States Council for International Business, Computer and Communications Industry Association, Engine), que incidia sobre a experiência das empresas certificadas no âmbito do QPD, em especial o processo de certificação, as medidas tomadas para cumprir os princípios do QPD, os mecanismos de tratamento de pedidos e queixas de cidadãos, etc.

[4] As reações recebidas podem ser consultadas na seguinte hiperligação: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14379-Quadro-UE-EUA-em-materia-de-privacidade-dos-dados-relatorio-da-Comissao-sobre-o-funcionamento-do-quadro_pt.

[5] A reunião de avaliação foi organizada por temas, sendo cada ponto específico da ordem de trabalhos introduzido por uma breve apresentação pela autoridade dos EUA, representante da UE ou organização pertinente, seguida de uma sessão aprofundada de perguntas e respostas. Os «aspetos comerciais» do quadro (ou seja, a aplicação e o cumprimento dos requisitos que incumbem às empresas certificadas no âmbito do QPD) foram abordados no primeiro dia, enquanto as questões relacionadas com o acesso do governo aos dados pessoais foram debatidas no segundo dia.

No que respeita à UE, a avaliação foi realizada por representantes da Direção-Geral da Justiça e dos Consumidores da Comissão Europeia, juntamente com cinco representantes designados pelo Comité Europeu para a Proteção de Dados (CEPD) e provenientes de diferentes autoridades nacionais de proteção de dados (APD) e da Autoridade Europeia para a Proteção de Dados[6]. Do lado dos EUA, participaram representantes do *Department of Commerce* (Ministério do Comércio, DoC), do *Department of State* (Ministério de Estado), da *Federal Trade Commission* (Comissão Federal do Comércio, FTC), do *Department of Transportation* (Ministério dos Transportes, DoT), do *Office of the Director of National Intelligence* (Gabinete do Diretor dos Serviços Nacionais de Informações, ODNI), do *Department of Justice* (Ministério da Justiça, DoJ), o *Inspector General for the Intelligence Community* (Inspetor-Geral do Setor das Informações), bem como membros da *Privacy and Civil Liberties Oversight Board* (Comissão de Controlo da Privacidade e das Liberdades Cívicas, PCLOB). Além disso, representantes de organizações que prestam serviços independentes de resolução de litígios e da *American Arbitration Association* (Associação Americana de Arbitragem) forneceram informações durante as sessões de avaliação pertinentes. Por outro lado, organizações certificadas no âmbito do QPD explicaram, por ocasião da reunião, a forma como as empresas cumprem os requisitos do quadro.

As conclusões da Comissão apoiaram-se ainda em material disponível ao público, tais como decisões judiciais, normas de execução e procedimentos das autoridades competentes dos EUA, relatórios e estudos de organizações não governamentais, relatórios de transparência publicados por empresas certificadas no âmbito do QPD, relatórios anuais de organismos de supervisão independentes, bem como notícias dos meios de comunicação social.

2. CONCLUSÕES

2.1. Aspetos comerciais

2.1.1. O processo de certificação

Para poder receber dados pessoais transferidos da UE com base no QPD, uma empresa dos EUA tem de certificar junto do DoC, e depois recertificar anualmente, a sua adesão a requisitos específicos em matéria de proteção de dados («princípios do QPD»). A certificação exige que a empresa esteja sujeita aos poderes de investigação e de execução da FTC ou do DoT, declare publicamente o seu compromisso de respeitar os princípios do QPD e divulgue publicamente a sua política em matéria de proteção da privacidade e aplique na íntegra esses requisitos[7]. Antes de finalizar uma certificação, o DoC verifica se a empresa cumpriu todos os requisitos de certificação[8].

Na reunião de avaliação, o DoC explicou que, neste primeiro ano do QPD, a prioridade tem sido estabelecer o processo de certificação, incluindo o desenvolvimento de ferramentas informáticas específicas, a atualização de procedimentos, o contacto com as empresas e a realização de outras atividades de divulgação/sensibilização. À data da reunião de avaliação, mais de 2 800 empresas tinham obtido a certificação no âmbito do QPD, o que significa que

[6] Os representantes da Comissão e do CEPD reuniram-se em 12 de junho e 10 de julho de 2024 para preparar a avaliação, debater os contributos recebidos e identificar os aspetos que exigem uma recolha de informações e esclarecimentos adicionais.

[7] Anexo I, secção I.2, da decisão de adequação.

[8] Anexo III da decisão de adequação.

mais empresas obtiveram a certificação no âmbito do QPD do que ao abrigo do quadro anterior, o Escudo de Proteção da Privacidade[9], no primeiro ano de funcionamento. De acordo com as informações fornecidas pelo DoC, 70 % dos participantes são PME e um grande número de empresas do QPD (47 %) pertencem ao setor das tecnologias de informação e comunicação (TIC). Além disso, 60 % das empresas estão certificadas exclusivamente para dados não relativos a recursos humanos, 2,5 % estão certificadas exclusivamente para dados relativos a recursos humanos e 37,5 % estão certificadas para ambos os tipos de dados.

O DoC adotou os procedimentos necessários para tratar os pedidos das empresas. Estas devem apresentar os seus pedidos de certificação no sítio Web do DoC relativo ao QPD (https://www.dataprivacyframework.gov/), que contém informações sobre a forma de aderir ao QPD[10] e sobre as obrigações da empresa ao abrigo do quadro[11]. Dentro do DoC, uma equipa específica, sob a tutela de um diretor dedicado ao Quadro de Privacidade de Dados, é responsável por todos os aspetos relacionados com a gestão e administração do QPD, incluindo o processo de certificação e o controlo da conformidade. Cada pedido é atribuído a um membro específico do pessoal que fica responsável pela empresa em causa ao longo de todo o processo de certificação.

Para efeitos de certificação no âmbito do quadro, as empresas apresentam o seu pedido, incluindo um projeto de política de privacidade. O DoC verifica se o pedido está em conformidade com os requisitos pertinentes do QPD. Quando as organizações pretendem certificar diferentes entidades dentro de um grupo de empresas (por exemplo, diversas filiais), o DoC solicita e analise uma política de privacidade abrangente que indique claramente todas as entidades a abranger ou, em alternativa, políticas separadas para cada entidade. O DoC verifica igualmente, junto do mecanismo de recurso independente[12] indicado no pedido, se a organização se registou efetivamente no mesmo. Para as empresas que selecionam o painel da autoridade de proteção de dados (por exemplo, porque tratam dados relativos a recursos humanos), o DoC verifica se a empresa pagou as taxas necessárias para recorrer ao painel. Se for caso disso, o DoC verifica igualmente se o requerente é abrangido pelo foro de competências da FTC ou do DoT (sendo, por conseguinte, elegível para aderir ao QPD).

Se todas as condições estiverem preenchidas, o DoC informa a organização de que pode publicar a sua política de privacidade referente ao QPD no seu sítio Web. Assim que a política de privacidade for pública, o DoC confirma a certificação e inscreve a empresa na lista do QPD no seu sítio Web. O QPD pode ser invocado para receber dados pessoais da UE a partir da data em que o DoC inscreve a organização nessa lista[13].

Tal como explicado na reunião de avaliação, os controlos efetuados até à data pelo DoC levaram à rejeição de 33 pedidos, por não cumprirem os requisitos do QPD. Regra geral, o DoC colabora com a empresa para corrigir eventuais deficiências. Se o DoC identificar deficiências, informa a empresa de que deve corrigi-las e que a ausência de resposta dentro de um determinado prazo, ou a não conclusão da sua autocertificação em conformidade com os

[9] No período equivalente, 2 400 empresas haviam obtido certificação no âmbito do Escudo de Proteção da Privacidade.

[10] https://www.dataprivacyframework.gov/program-articles/How-to-Join-the-Data-Privacy-Framework-(DPF)-Program-(part%E2%80%931).

[11] https://www.dataprivacyframework.gov/key-requirements.

[12] Mecanismos de resolução de litígios do setor privado através dos quais as queixas e os litígios dos cidadãos são investigados e resolvidos de forma célere sem custos para os cidadãos.

[13] Anexo I, secção I, n.º 3, da decisão de adequação.

procedimentos do DoC, levará a que o seu pedido seja considerado rejeitado. Se a certificação inicial não for concluída/alterada no prazo de 12 meses, o DoC considera-a rejeitada.

A data limite para a renovação da certificação anual é especificada na lista do QPD para cada empresa. Para recordar às empresas a necessidade de solicitar a renovação da certificação, o DoC criou um sistema com lembretes de que a certificação está prestes a expirar. As organizações recebem um lembrete um mês antes, duas semanas antes e um dia antes da data limite. As empresas que deixam caducar a sua certificação são suprimidas da lista do QPD. Tal como descrito no anexo III da decisão de adequação, o DoC tem uma secção específica no seu sítio Web que enumera as organizações dos EUA que deixaram de ser participantes ativos e identifica as razões (por exemplo, caducidade ou retirada) pelas quais as empresas em causa foram suprimidas da lista (a «lista inativa»). Quando as organizações são suprimidas da lista do QPD por terem deixado caducar a sua certificação, o DoC contacta-as para confirmar se pretendem retirar-se ou se tencionam renovar a certificação e, em caso afirmativo, verificar se, durante o tempo em que o seu estatuto de certificação esteve caducado, aplicaram os princípios do QPD aos dados pessoais recebidos no âmbito do QPD e esclarecer que medidas tomarão para resolver as questões pendentes que conduziram ao retardamento da sua renovação da certificação. Quando as empresas notificam o DoC de que pretendem retirar-se do QPD, o DoC exige que confirmem se irão devolver ou apagar os dados recebidos no âmbito do QPD; mantê-los e continuar a aplicar os princípios do QPD a esses dados (o que tem de ser confirmado anualmente); ou mantê-los e aplicar outras proteções (tais como cláusulas contratuais-tipo adotadas pela Comissão Europeia).

As reações recebidas de associações comerciais e empresas indicam que as empresas certificadas no âmbito do QPD tomaram uma série de medidas para garantir o cumprimento dos princípios do QPD. Por exemplo, para cumprir o *princípio de recurso, aplicação e responsabilidade*, as organizações realizaram controlos internos, quer através de autoavaliação, quer através de uma verificação de conformidade externa. Os dois mecanismos de recurso independentes do setor privado que participaram na reunião de avaliação explicaram que também disponibilizam uma verificação de conformidade externa através da avaliação das políticas de privacidade, e um dos mecanismos explicou que também disponibiliza auditorias e controlos aleatórios, centrando-se, por exemplo, nos princípios de *acesso*, *escolha* e *transferência ulterior*. Além disso, as empresas certificadas elaboraram programas de conformidade interna e mecanismos de supervisão, ministraram formação a trabalhadores, implementaram mecanismos para permitir que os cidadãos exerçam os seus direitos, efetuaram avaliações do impacto na privacidade e analisaram os contratos existentes.

2.1.2. Controlo do cumprimento, falsas alegações de adesão e aplicação

No âmbito do QPD, o DoC é responsável pelo controlo do cumprimento dos princípios do QPD através da utilização de diferentes instrumentos, incluindo controlos *ex officio* (por sua própria iniciativa), controlos esporádicos *ad hoc* e questionários de conformidade. Tal inclui a pesquisa e o tratamento de falsas alegações de adesão ao quadro, por exemplo através de pesquisas na Internet[14].

Para controlar o cumprimento dos princípios pelas empresas que aderem ao QPD, o DoC baseou-se principalmente em pesquisas Web *ad hoc* e em verificações na comunicação social

[14] Ver anexo III da decisão de adequação. Podem surgir falsas alegações, por exemplo, quando uma empresa alega participar no QPD sem nunca ter iniciado o processo de certificação ou, tendo-o iniciado, não o concluiu ou deixou caducar a sua certificação.

(redes sociais) ao longo do último ano. O DoC comunicou que não detetou problemas de cumprimento dos princípios do QPD neste primeiro ano e não indicou quaisquer empresas à FTC ou ao DoT para a aplicação de eventuais medidas coercivas. Criou igualmente um ponto de contacto específico para facilitar a cooperação com as APD e receber queixas de particulares e consultas de outras autoridades (por exemplo, APD ou a FTC). No entanto, não foram recebidas consultas ou queixas durante o ano transato. Enquanto este primeiro ano de funcionamento do QPD se centrou na criação do quadro e do processo de certificação, o DoC explicou, na reunião de avaliação, que tenciona realizar controlos de conformidade por meios automatizados, a fim de os realizar de forma mais sistemática, e está atualmente a desenvolver as ferramentas informáticas necessárias para o efeito.

A Comissão reconhece que o DoC teve de concentrar os seus esforços neste primeiro ano na criação do quadro e do processo de certificação. Futuramente, é importante que o DoC intensifique os seus esforços para acompanhar e verificar o cumprimento dos princípios, o que é necessário para assegurar um nível elevado e contínuo de conformidade com o quadro e detetar casos que exijam novas medidas coercivas, incluindo eventuais falsas alegações de adesão das empresas. A este respeito, a Comissão congratula-se com o facto de o DoC ter confirmado a sua intenção de criar e utilizar instrumentos (automatizados) para identificar de forma mais eficaz e sistemática problemas de cumprimento e falsas alegações, e considera que tal deve estar integrado num esforço mais vasto para um maior recurso aos diferentes instrumentos à sua disposição (por exemplo, controlos esporádicos, questionários de verificação da conformidade, pedidos de informação, etc.), incluindo para verificar o cumprimento de requisitos específicos ao abrigo do QPD[15].

As organizações do QPD estão sujeitas à jurisdição da FTC e do DoT. Durante a reunião de avaliação, o DoT confirmou que dispõe de todos os processos para tomar medidas coercivas adequadas. Explicou igualmente que muito poucas empresas sob a sua jurisdição aderiram ao QPD (ou seja, algumas agências de viagens, mas nenhuma companhia aérea). A FTC confirmou que verifica sistematicamente as violações do QPD em cada uma das suas investigações em matéria de privacidade. Até à data, a FTC não recebeu consultas de outras autoridades. Recebeu algumas queixas que mencionavam o QPD, embora duas dissessem respeito a empresas incluídas na «lista inativa», duas respeitassem a empresas que não participavam no quadro e uma não estivesse relacionada com dados pessoais transferidos da UE. À data do presente relatório, a FTC não tinha emitido decisões para impor o cumprimento do QPD, embora tenha confirmado que várias empresas certificadas no âmbito do QPD estão atualmente a ser investigadas.

A Comissão congratula-se com o facto de a FTC verificar sistematicamente as violações do QPD em todas as suas investigações em matéria de privacidade. Uma vez que a eficácia contínua do QPD depende da sua aplicação rigorosa, espera-se que a FTC continue a exercer os seus poderes de investigação no âmbito do quadro, nomeadamente através da realização proativa de ações de fiscalização centradas no cumprimento dos requisitos específicos do QPD e/ou de determinados setores.

2.1.3. Tratamento das queixas

[15] Por exemplo, no que diz respeito às transferências ulteriores, recorrendo à possibilidade, nos termos do princípio 3, alínea b), de solicitar um resumo ou uma cópia representativa das disposições pertinentes dos contratos em matéria de privacidade para as transferências ulteriores.

O QPD proporciona aos cidadãos da UE diferentes possibilidades de recurso em casos de incumprimento dos princípios do QPD por parte de organizações certificadas[16]. Inclui a prossecução da resolução através de contactos diretos com uma organização do QPD, que deve dar uma resposta ao cidadão afetado no prazo de 45 dias. Os cidadãos podem igualmente apresentar uma queixa a um mecanismo de recurso independente designado por uma organização para investigar e resolver queixas. Dependendo das circunstâncias, pode tratar-se de um organismo de resolução alternativa de litígios ou de uma APD[17]. Por último, no caso de nenhuma das outras vias de recurso disponíveis ter resolvido satisfatoriamente a queixa do titular dos dados, os cidadãos podem acionar a arbitragem vinculativa perante o Comité do QPD UE-EUA enquanto mecanismo de último recurso.

2.1.3.1. Tratamento de queixas pelas empresas

As respostas das associações comerciais e das empresas aos questionários enviados pela Comissão indicam que as empresas certificadas no âmbito do QPD receberam muito poucas, ou nenhumas, queixas de cidadãos relativas ao incumprimento dos princípios do QPD. Ao mesmo tempo, as empresas criaram diferentes mecanismos e ferramentas para permitir que os cidadãos exerçam os seus direitos e apresentem queixas, nomeadamente através de formulários em linha, correio eletrónico e telefone.

2.1.3.2. *Mecanismos de recurso independentes*

As reações recebidas durante a reunião de avaliação e as informações facultadas pelas associações comerciais indicam que houve um número muito reduzido de queixas apresentadas a mecanismos de resolução independentes. Os mecanismos de recurso independentes selecionados pelas empresas incluem a BBB National Programs, JAMS, TRUSTe e VeraSafe. O QPD exige que os mecanismos de recurso independentes publiquem um relatório anual com estatísticas agregadas sobre a utilização dos seus serviços de resolução de litígios. Aquando da adoção do presente relatório, todos mecanismos de recurso independentes em causa tinham publicado os seus relatórios anuais[18].

Além disso, na reunião de avaliação, a BBB e a VeraSafe fizeram apresentações pormenorizadas sobre as suas atividades relativas ao ano anterior. Comunicaram um aumento,

---

[16] Ver secção 2.4 da decisão de adequação.

[17] As organizações do QPD são obrigadas a cooperar na investigação e na resolução de uma queixa apresentada 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.

[18] ANA — https://www.ana.net/content/show/id/accountability-dpf-consumers;
BBB National Programs — https://assets.bbbprograms.org/docs/default-source/eu-privacy-shield/dpf_periodicalreport_072024.pdf; ICDR – AAA — https://go.adr.org/rs/294-SFS-516/images/Data%20Privacy%20Framework%20IRM%20Program%20Report%202023-2024%20FINAL.pdf?version=0;
Insights association — https://www.insightsassociation.org/Portals/INSIGHTS/Insights%20Association%20DPF%20Services%20Program%202024%20Annual%20Report_Final_1.pdf;
JAMS — https://www.jamsadr.com/files/Uploads/Documents/2024-Annual-Report-DPF-Cases.pdf;
Privacy Trust DPF Services — https://privacytrust.com/fserve/PrivacyTrust_Dispute_Resolution_Report_2023_2024.pdf;
TRUSTe Dispute Resolution — https://trustarc.com/wp-content/uploads/2024/07/2024-Independent-Recourse-Mechanism-Annual-Report.pdf;
Verasafe — https://verasafe.com/wp-content/uploads/2020/06/VeraSafe-DPF-Dispute-Resolution-Program-Annual-Report-2024.pdf.

em comparação com quadros anteriores, do número de participantes que são empresas que escolheram os seus serviços e referiram que tinham recebido algumas queixas, embora a grande maioria fosse inelegível. Por exemplo, a BBB recebeu 87 queixas de cidadãos da UE, sendo apenas duas delas elegíveis para resolução. Embora a BBB tenha explicado que as queixas são, em média, tratadas no prazo de cinco dias úteis, estas duas queixas acabaram por ser encerradas devido à falta de resposta dos cidadãos. A VeraSafe recebeu 26 queixas, seis das quais elegíveis para resolução. Duas diziam respeito a pedidos de acesso e de eliminação e foram resolvidas, duas continuam pendentes e duas foram retiradas ou encerradas devido à falta de resposta do cidadão. Ambos os mecanismos de recurso independentes explicaram que procuram responder às queixas na língua do cidadão.

As empresas do QPD que tratam dados de recursos humanos transferidos da UE devem selecionar as APD da UE como seu mecanismo de recurso independente para esses dados, ao passo que uma empresa do QPD pode, a título voluntário, selecionar as APD da UE como seu mecanismo de recurso independente para outros tipos de dados pessoais transferidos com base no QPD. Com efeito, mais de metade das empresas certificadas no âmbito do QPD à data da avaliação optaram por esta solução[19], o que é de saudar. Desde a adoção da decisão de adequação, o CEPD adotou o regulamento interno do «painel informal de APD da UE». O painel é competente para prestar aconselhamento vinculativo às organizações dos EUA na sequência de queixas não resolvidas relacionadas com o QPD, apresentadas por cidadãos sobre o tratamento de dados pessoais transferidos da UE no âmbito do QPD. De acordo com o seu regulamento interno, o painel é constituído por uma APD que atua como APD principal e por outras APD coavaliadoras designadas[20]. Presta aconselhamento vinculativo no prazo de 60 dias a contar da receção de uma queixa relacionada com o QPD. O CEPD publicou igualmente um modelo de formulário para a apresentação de queixas às APD[21], bem como perguntas frequentes para os cidadãos[22] e as empresas europeus[23] sobre o QPD. No momento da avaliação, o painel não tinha recebido qualquer queixa.

2.1.3.3. Mecanismo de arbitragem de caráter vinculativo

O *International Centre for Dispute Resolution* (Centro Internacional de Resolução de Litígios) (ICDR), que é a divisão internacional da *American Arbitration Association*, foi selecionado pelo DoC para administrar o mecanismo de arbitragem de caráter vinculativo. Na sequência da adoção da decisão de adequação, o DoC, juntamente com a Comissão, selecionou 11 árbitros com experiência em matéria de privacidade e oriundos de vários contextos, incluindo a arbitragem, o poder judicial, o meio académico e a sociedade civil[24]. Além disso, foram adotadas as regras de arbitragem[25] para o Comité do QPD e um código de conduta para os

[19] Pouco depois da data da reunião de avaliação, o sítio Web do QPD indicou que 1 511 dos 2 892 participantes tinham uma Autoridade de Proteção de Dados da UE como seu mecanismo de recurso.
[20] Em 17 de abril de 2024, o CEPD adotou o regulamento interno do «painel informal de APD da UE», de acordo com o Quadro de Privacidade de Dados UE-EUA. Pode ser consultado no seguinte endereço: https://www.edpb.europa.eu/system/files/2024-04/dpf_rules-of-procedure_informal-panel-dpas_en.pdf.
[21] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/eu-us-data-privacy-framework-template-complaint-form_pt.
[22] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/eu-us-data-privacy-framework-faq-european-individuals_pt.
[23] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/eu-us-data-privacy-framework-faq-european-businesses_pt.
[24] https://go.adr.org/DPF_Arbitrator_Bios.html.
[25] https://go.adr.org/rs/294-SFS-516/images/IC.DR-AAA_EU-US_DPF_AnnexI_Arbitration_Rules.pdf.

árbitros[26], que estão disponíveis no sítio Web do ICDR. À data da avaliação, o mecanismo de arbitragem ainda não tinha sido acionado por cidadãos da UE.

2.1.4. Orientação, cooperação e sensibilização

Desde a entrada em vigor do QPD, o DoC tem levado a cabo várias atividades de sensibilização através da organização de campanhas itinerantes, de webinários e de conferências, do contacto com associações comerciais e da interação direta com mais de 3 000 empresas para fornecer informações sobre o QPD. Publicou igualmente orientações, nomeadamente sob a forma de perguntas frequentes que se destinam aos cidadãos, bem como a empresas da UE e dos EUA[27]. Por sua vez, o CEPD elaborou formulários de apresentação de queixas e perguntas frequentes que se destinam a cidadãos e empresas. Do mesmo modo, a Comissão publicou perguntas e respostas e uma ficha informativa sobre o QPD quando adotou a sua decisão de adequação[28].

Ao mesmo tempo, a reunião de avaliação revelou que são necessários esforços suplementares para sensibilizar os cidadãos e fornecer orientações às empresas. Os contributos recebidos das empresas e dos mecanismos de recurso independentes e o número muito reduzido de queixas sugerem que os cidadãos podem nem sempre estar cientes dos seus direitos e/ou do mecanismo para os exercer. Durante a reunião de avaliação, o DoC manifestou interesse em colaborar com as APD da UE para aumentar a sensibilização dos cidadãos da UE em relação ao quadro. A Comissão incentiva essas iniciativas e está também a tomar medidas para informar melhor os cidadãos, nomeadamente ao disponibilizar informações adicionais sobre o QPD no seu sítio Web, por exemplo, incorporando ligações e referências a documentos de orientação pertinentes adotados pelo CEPD, pelo DoC e por outras autoridades dos EUA.

No que respeita às orientações sobre os princípios do QPD, os representantes do CEPD acordaram, durante a reunião de avaliação, cooperar nos próximos meses para prestar esclarecimentos adicionais sobre o conceito de dados de recursos humanos no âmbito do QPD e as obrigações específicas aplicáveis ao tratamento desses dados. Foram explorados diferentes elementos a incluir nessas orientações. Por exemplo, poderiam abordar determinados cenários práticos em que os dados relativos aos trabalhadores seriam tratados ao abrigo do QPD (por exemplo, por um prestador de serviços de computação em nuvem) e explicar, nesses cenários, quais as obrigações do QPD que seriam pertinentes. Além disso, poderiam sugerir às empresas que recebem dados relativos a cidadãos da UE enquanto trabalhadores (mas que não utilizam necessariamente esses dados no contexto de uma relação laboral) que escolham o painel das APD como seu instrumento de recurso independente. Tal asseguraria que esses cidadãos possam dirigir-se a uma autoridade «próxima no seu país» e, se for caso disso, mais familiarizada com a legislação nacional aplicável aos dados de recursos humanos.

Além disso, um aspeto específico em que parece ser útil mais orientações (também com base nos contributos recebidos de associações comerciais) diz respeito aos requisitos do QPD para as transferências ulteriores. Além disso, o DoC indicou que seria oportuno analisar se alguns setores poderiam beneficiar de orientações adicionais sobre a aplicação dos princípios do QPD

[26] https://go.adr.org/rs/294-SFS-516/images/Code_of_Conduct_for_Arbitrators_Appointed_to_EU-US_DPF_AnnexI_Arbitrations.pdf.

[27] Ver, por exemplo, https://www.dataprivacyframework.gov/US-Businesses.

[28] https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/eu-us-data-transfers_en.

às suas atividades, por exemplo, na área da investigação no domínio da saúde e dos serviços financeiros.

A Comissão congratula-se com a disponibilidade de ambas as partes para elaborar orientações e espera que os trabalhos sobre os temas acima referidos tenham início em breve.

De um modo mais geral, foram criados vários mecanismos para assegurar o intercâmbio e a cooperação entre as autoridades dos EUA e as APD, nomeadamente através da nomeação de pontos de contacto específicos na FTC e no DoC para tratar os pedidos de informação e as consultas submetidas pelas APD.

2.1.5. Desenvolvimentos relevantes no sistema jurídico dos EUA

Desde a adoção da decisão de adequação, verificou-se uma série de desenvolvimentos no quadro jurídico dos EUA no domínio da privacidade, nomeadamente a nível legislativo, regulamentar e jurisprudencial. De um modo geral, assinalam uma maior convergência entre as abordagens da UE e dos EUA em relação a determinados desafios em matéria de privacidade, nomeadamente através da utilização de conceitos jurídicos semelhantes. Alguns destes desenvolvimentos estão em curso e terão de ser objeto de um acompanhamento mais aprofundado.

A nível federal, o presidente emitiu vários *executive orders* (decretos presidenciais) relevantes para a utilização de dados pessoais. Em especial, o *Executive Order 14117*, de 28 de fevereiro de 2024[29], proíbe ou limita as transações que envolvam determinadas categorias de dados pessoais sensíveis (por exemplo, dados de saúde, identificadores biométricos, dados genómicos humanos) com entidades de alguns «países que suscitam preocupação»[30]. O decreto adotado encarrega o Procurador-Geral de propor regulamentos — ainda por emitir no momento da adoção do presente relatório — para especificar melhor a sua aplicação. Além disso, o *Executive Order 14110*, de 30 de outubro de 2023, relativo à inteligência artificial[31] centra-se no desenvolvimento de uma inteligência artificial segura, protegida e fiável. Exige que várias agências federais elaborem normas e orientações de segurança relacionadas com a IA, nomeadamente sobre riscos específicos da IA para a privacidade e sobre técnicas de preservação da privacidade.

Em termos de trabalho legislativo, embora nos últimos anos tenham sido apresentados no Congressos projetos de lei relativos à privacidade, houve 20 estados dos EUA que, em julho de 2024, adotaram leis abrangentes em matéria de privacidade, das quais oito entraram em vigor: Califórnia, Colorado, Oregon, Virgínia, Connecticut, Utah, Texas e Florida. Além disso, 17 estados dos EUA adotaram legislação que aborda o tratamento automatizado (ou, pelo menos,

[29] https://www.federalregister.gov/documents/2024/03/01/2024-04573/preventing-access-to-americans-bulk-sensitive-personal-data-and-united-states-government-related.

[30] Entre estes incluem-se, tal como proposto pelo Procurador-Geral num Aviso prévio da proposta de regulamentação, emitido em 3 de maio de 2024, a China, Cuba, Hong Kong e Macau, o Irão, a Coreia do Norte e a Venezuela. Ver https://www.federalregister.gov/documents/2024/03/05/2024-04594/national-security-division-provisions-regarding-access-to-americans-bulk-sensitive-personal-data-and.

[31] https://www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence.

algumas das suas formas) e permite, de um modo geral, a autoexclusão relativamente a certos tipos de tomada de decisões com base na «definição de perfis»[32].

Em termos de evolução da jurisprudência, vários representantes da sociedade civil chamaram a atenção para o recente acórdão do Supremo Tribunal dos EUA no processo Loper Bright Enterprises v. Raimondo (de 28 de junho de 2024). Este acórdão põe em causa a jurisprudência anterior sobre a doutrina Chevron, segundo a qual os tribunais aplicam o princípio da deferência à interpretação razoável da lei por parte de uma entidade reguladora, em caso de ambiguidade numa lei aplicada por essa entidade reguladora. Em especial, algumas ONG manifestaram preocupações quanto ao impacto deste acórdão do Supremo Tribunal na autoridade de regulamentação da FTC no domínio da privacidade, embora reconheçam que o impacto sobre os seus poderes de execução pode ser nulo ou limitado. Na reunião de avaliação, a FTC informou que ainda é cedo para conhecer as implicações exatas deste acórdão. Ao mesmo tempo, explicou que a regulamentação da FTC é efetuada sob uma autoridade prevista na *FTC Act*, diferente da de outros organismos administrativos e para a qual a doutrina Chevron era menos relevantes. O acórdão recente pode, por conseguinte, ter um impacto limitado neste domínio.

Além disso, a FTC prestou informações sobre a evolução recente da sua abordagem ao tratamento automatizado e à inteligência artificial. Inclui a adoção de uma declaração conjunta, juntamente com outras autoridades responsáveis pela aplicação da lei, contra a discriminação e os preconceitos nos sistemas automatizados[33], bem como várias medidas coercivas — em que a FTC se centra, nomeadamente, na transparência, na equidade do tratamento automatizado e na capacidade de os cidadãos contestarem os resultados. O caso mais importante a este respeito é a decisão da FTC contra a Rite Aid, em março de 2024, que aplicou à empresa uma proibição de utilizar, durante cinco anos, a tecnologia de reconhecimento facial para fins de segurança[34]. Em especial, a FTC concluiu que a Rite Aid não tomou medidas razoáveis para evitar resultados errados e informar os consumidores sobre a tecnologia utilizada. De um modo mais geral, na reunião de avaliação, a FTC abordou as suas prioridades atuais e, nomeadamente, os domínios que, na sua opinião, merecem uma abordagem de aplicação mais proativa no futuro, incluindo a proteção de dados sensíveis (por exemplo, dados de saúde,

[32] Embora existam diferenças no que se refere ao significado de «definição de perfis» entre os diversos estados, a definição de perfis é geralmente definida como qualquer forma de tratamento automatizado de dados pessoais para avaliar, analisar ou prever aspetos pessoais relacionados com a situação económica, a saúde, as preferências pessoais, os interesses, a fiabilidade, o comportamento, a localização ou os movimentos de uma pessoa singular identificada ou identificável. Normalmente, são os consumidores que podem autoexcluir-se da definição de perfis. Os seguintes estados elaboraram legislação sobre a definição de perfis: Colorado (Colo. Estat. Rev. Anot. § 6-1-1306), Connecticut (Conn. Estat. Gen. Anot. § § 42-518), Delaware (Del. 6, § 12D-104), Florida (Fla. Estat. Anot. § 501.705), Indiana (Código Ind. Anot. § 24-15-3-1), Kentucky (Ky. Estat. Rev. Anot. § 367.3615), Maryland [*Maryland Online Data Privacy Act* (Lei de Maryland relativa à privacidade dos dados em linha) de 2024, aprovada em 9 de maio de 2024], Minnesota (Minn. Estat. Anot. § 325O.07), Montana (Mont. § 30-14-2808), Nebrasca (Neb. Estat. Rev. Anot. § 87-1107), Nova Hampshire (N.H. Estat. Rev. Anot. § 507-H:4), Nova Jérsia (N.J. Estat. Anot. § 56:8-166.8), Oregon (Or. Estat. Rev. Anot. § 646A.574), Rhode Island [*Rhode Island Data Transparency and Privacy Protection Act* (Lei relativa à transparência dos dados e à proteção da privacidade de Rhode Island), aprovada em 29 de junho de 2024], Tennessee (Tenn. Código anot. § 47-18-3304), Texas (Tex. Código das Empresas e Com. Anot. § 541.051), e Virgínia (Va. Código Anot. § 59.1-577).

[33] https://files.consumerfinance.gov/f/documents/cfpb_joint-statement-enforcement-against-discrimination-bias-automated-systems_2023-04.pdf.

[34] https://www.ftc.gov/legal-library/browse/cases-proceedings/2023190-rite-aid-corporation-ftc-v.

dados biométricos, geolocalização)[35], a proteção de crianças[36] e menores em linha e a segurança dos dados[37].

A Comissão continuará a acompanhar de perto estes e outros desenvolvimentos nos EUA, em especial quaisquer novas medidas no sentido de uma lei federal abrangente em matéria de privacidade e o possível impacto da recente jurisprudência do Supremo Tribunal sobre o papel da FTC no domínio da privacidade.

A Comissão congratula-se com as informações fornecidas pela FTC sobre as suas recentes atividades de aplicação da legislação e as prioridades atuais que correspondem, em grande medida, às tendências e prioridades em matéria de aplicação da proteção de dados na Europa. A FTC participa também ativamente na rede que reúne países que beneficiam de uma decisão de adequação da UE, lançada pela Comissão em março de 2024[38]. Esta maior convergência deverá incentivar e facilitar uma cooperação mais estreita entre as autoridades de proteção da privacidade em ambos os lados do Atlântico, nomeadamente em questões pertinentes para o funcionamento do QPD.

2.2. Aspetos relacionados com o acesso e a utilização de dados pessoais transferidos no âmbito do Quadro de Privacidade de Dados UE-EUA pelas autoridades públicas dos EUA

A decisão de adequação contém uma avaliação pormenorizada das regras que regem a recolha e a utilização de dados pessoais transferidos da UE para empresas certificadas no âmbito do QPD pelas autoridades públicas dos EUA, em especial para efeitos de aplicação do direito penal e de segurança nacional. Desde a adoção da decisão de adequação, tal como confirmado pelas autoridades dos EUA durante a reunião de avaliação, não se registaram, no primeiro ano do QPD, quaisquer desenvolvimentos relevantes no que diz respeito ao quadro jurídico aplicável ao acesso aos dados para fins regulamentares ou de aplicação da lei. Por este motivo, as conclusões que se seguem dizem apenas respeito à evolução no domínio da segurança nacional.

As conclusões da decisão de adequação sobre o acesso aos dados pelos serviços de informações baseiam-se na análise das condições e limitações aplicáveis às operações de informação de origem eletromagnética ao abrigo de várias autoridades jurídicas competentes — em especial a secção 702 da *Foreign Intelligence Surveillance Act* (Lei de Vigilância de Informações

[35] Ver, por exemplo, o recente despacho da FTC contra a X-Mode pela venda e partilha de informações sensíveis sobre a localização (https://www.ftc.gov/system/files/ftc_gov/pdf/X-ModeSocialDecisionandOrder.pdf) e contra a Monument relativamente à divulgação a terceiros de dados sensíveis relativos à saúde para efeitos de comercialização (https://www.ftc.gov/system/files/ftc_gov/pdf/MonumentOrderFiled.pdf).

[36] Por exemplo, a FTC anunciou recentemente uma investigação conducente a uma ação judicial contra a TikTok e a sua empresa-mãe, a Bytedance, por alegada violação da legislação em matéria de privacidade das crianças. Alega-se que ambas as empresas não cumpriram a obrigação de notificar e obter o consentimento dos pais antes de recolherem e utilizarem informações pessoais de crianças com menos de 13 anos (https://www.ftc.gov/news-events/news/press-releases/2024/08/ftc-investigation-leads-lawsuit-against-tiktok-bytedance-flagrantly-violating-childrens-privacy-law).

[37] Ver síntese das recentes atividades de aplicação da legislação na Atualização de 2023 sobre Privacidade e Segurança dos Dados da FTC: https://ec.europa.eu/commission/presscorner/detail/en/mex_24_1307.

[38] Ver https://ec.europa.eu/commission/presscorner/detail/en/mex_24_1307. Na sequência da reunião de março de 2024, foi decidido realizar uma série de sessões temáticas. A primeira teve lugar em julho de 2024 e centrou-se na criação de instrumentos que possam ajudar as pequenas e médias empresas a cumprir a legislação em matéria de privacidade.

Externas) (FISA) e o *Executive Order 12333*[39] — tal como complementados e reforçados pelo *Executive Order 14086*relativo ao reforço das salvaguardas para as atividades de recolha de informações de origem eletromagnética dos Estados Unidos (EO 14086), adotado pelo presidente dos EUA em 7 de outubro de 2022. As salvaguardas estabelecidas no EO 14086 aplicam-se a todas as atividades de informação de origem eletromagnética dos EUA, independentemente da autoridade jurídica em que essas atividades se baseiam e do local onde ocorrem, e protegem os dados de cidadãos de países terceiros (incluindo europeus)[40]. O EO 14086 também estabeleceu um novo mecanismo de recurso através do qual estas garantias vinculativas podem ser invocadas e aplicadas pelos cidadãos na UE.

As secções seguintes descrevem as medidas tomadas pelas autoridades dos EUA desde a adoção da decisão de adequação para dar cumprimento ao EO 14086, bem como os desenvolvimentos pertinentes a nível do quadro jurídico acima referido.

2.2.1. Desenvolvimentos relevantes no que respeita ao quadro jurídico dos EUA

2.2.1.1. Aplicação do Executive Order 14086 *pelos serviços de informações*

As limitações e salvaguardas introduzidas pelo EO 14086 complementam as previstas na secção 702 do FISA e no EO 12333. São vinculativas para todos os serviços de informações e foram ainda mais operacionalizadas através de políticas e procedimentos adotados por cada serviço.

No âmbito da primeira avaliação, as autoridades dos EUA confirmaram que não houve alterações ao EO 14086 desde a sua adoção. Além disso, foi clarificado que o presidente dos EUA não fez uso do poder previsto nas secções 2(b)(i)(B) e 2(b)(ii)(C) do EO 14086 para atualizar a lista de objetivos legítimos para os quais pode ser utilizada a informação de origem eletromagnética ou a lista de finalidades para as quais os dados recolhidos em larga escala podem ser utilizados[41]. Para determinar as prioridades em matéria de informações mais específicas para as quais pode efetivamente ser recolhida informação de origem eletromagnética , o EO 14086 criou um procedimento específico. Em especial, o *Civil Liberties Protection Officer* (agente responsável pela proteção das liberdades cívicas) do ODNI (CLPO do ODNI) deve ser consultado para avaliar, em relação a cada prioridade, se 1) promove um ou mais objetivos legítimos enumerados no EO, 2) não foi concebida nem prevista para resultar na recolha de informação de origem eletromagnética para um objetivo proibido enumerado no EO e 3) foi criada após uma análise adequada da privacidade e das liberdades cívicas de todas as pessoas[42]. O CLPO do ODNI confirmou, durante a reunião de avaliação, que examinou as prioridades propostas pelo diretor dos serviços nacionais de informações *(Director of National Intelligence)* no *National Intelligence Priorities Framework* (quadro das prioridades dos

[39] Outras medidas que podem ser tomadas no âmbito da FISA no que respeita aos dados transferidos da UE são a vigilância eletrónica individualizada (secção 105 da FISA), as buscas físicas (secção 302 da FISA), a utilização de dispositivos de registo de chamadas telefónicas e comunicações eletrónicas (secção 402 da FISA) e a recolha de registos comerciais de determinadas empresas (empresas de transportes públicos, unidades de alojamento públicas, estabelecimentos de aluguer de veículos ou estabelecimentos de armazenamento, secção 501 da FISA). Estas diferentes bases jurídicas são analisadas em pormenor na decisão de adequação (considerandos 142 a 152).

[40] Para mais informações, consultar a secção 3.2.1.2 da decisão de adequação.

[41] Estes objetivos/finalidades legítimos incluem, por exemplo, a proteção contra a espionagem, a sabotagem, o assassinato ou outras atividades de informações levadas a cabo por, em nome de, ou com a assistência de um governo, organização ou cidadão estrangeiros; proteção contra o terrorismo, a tomada de reféns e a manutenção de pessoas em cativeiro por um governo, organização ou cidadão estrangeiros ou em seu nome.

[42] Secção 2(b)(iii) do EO 14086.

serviços de informações nacionais) de 2023 e concluiu que cumpriam os requisitos acima referidos, tendo partilhado a sua conclusão com o diretor dos serviços nacionais de informações, que, por sua vez, apresentou as prioridades ao presidente para validação. O CLPO do ODNI também ofereceu formação sobre os requisitos do EO 14086 a partes da comunidade de informações envolvidas na elaboração de prioridades em matéria de informações.

Além disso, no ano passado, as autoridades dos EUA tomaram novas medidas práticas para aplicar o EO 14086 nas suas operações quotidianas. Em especial, os serviços de informações estabeleceram novas políticas e orientações internas sobre a aplicação do OE, por exemplo, processos internos (através de requisitos de autorização interna, controlos de acesso documentados, para que apenas as pessoas que receberam formação adequada e que possuam os requisitos necessários para a missão tenham acesso às informações, etc.), a fim de assegurar o cumprimento dos requisitos de necessidade e de proporcionalidade, tanto no contexto da recolha seletiva como da recolha em larga escala[43]. Além disso, foi ministrada formação sobre o EO 14086 ao pessoal de diferentes serviços de informações (por exemplo, NSA, CIA, FBI), incluindo sessões de formação anuais e *ad hoc* organizadas pelo CLPO do ODNI e formações obrigatórias para todos os novos membros que integrem o ODNI.

A Comissão congratula-se com as várias medidas adotadas para aplicar e garantir o cumprimento do EO 14086. À medida que é adquirida mais experiência com a aplicação prática das salvaguardas do EO, em futuras avaliações a Comissão apreciaria a oportunidade de debater exemplos concretos da forma como o EO é aplicado na prática (respeitando as considerações de confidencialidade aplicáveis).

2.2.1.2. Renovação da autorização prevista na secção 702 da FISA

A secção 702 da FISA permite que se visem cidadãos de países terceiros que se acredita estarem localizados fora dos Estados Unidos a fim de obter informações no estrangeiro. A obtenção é efetuada com base em certificações anuais apresentadas e aprovadas pelo *Foreign Intelligence Surveillance Court* (tribunal encarregado de supervisionar os pedidos e mandatos em matéria de vigilância — FISC). Estas certificações identificam categorias específicas de informações externas a recolher. Em 21 de julho de 2023, o ODNI anunciou a existência de três certificações aprovadas ao abrigo da secção 702 da FISA, que abrangem as seguintes categorias de informações externas: 1) governos estrangeiros e entidades conexas, 2) luta contra o terrorismo e 3) luta contra a proliferação[44]. As certificações devem também incluir procedimentos de seleção de alvos e minimização aprovados pelo FISC[45]. Em especial, a seleção de alvos é efetuada solicitando que as empresas americanas que correspondem à definição da FISA de «prestador de serviços de comunicações eletrónicas» divulguem dados de comunicações eletrónicas relativos a comunicações enviadas para ou a partir de «seletores», que identifiquem uma conta de comunicação específica, por exemplo, um número de telefone ou um endereço de correio eletrónico. O Governo dos EUA publicou uma série de materiais sobre a secção 702

[43]Ver https://www.intel.gov/ic-on-the-record-database/results/oversight/1278-odni-releases-ic-procedures-implementing-new-safeguardsin-executive-order-14086, publicado em 3 de julho de 2023.
[44] https://www.intelligence.gov/ic-on-the-record-database/results/1307-release-of-documents-related-to-the-2023-fisa-section-702-certifications.
[45] Esses procedimentos limitam a recolha de dados no que diz respeito a uma finalidade específica de informações externas, restringem o acesso a bases de dados em que são armazenadas as informações obtidas ao abrigo da secção 702 da FISA (incluindo através de controlos de acesso) e impõem limites à utilização, conservação e divulgação dessas informações.

da FISA para informar o público sobre o funcionamento dos programas de vigilância, os requisitos aplicáveis e a proteção da privacidade, bem como sobre o papel do FISC[46].

Devido a uma cláusula de caducidade, a secção 702 da FISA deveria expirar no final de 2023, a menos que fosse novamente autorizada pelo Congresso. Após uma nova autorização temporária sem quaisquer alterações, o Congresso aprovou a *Reforming Intelligence and Securing America Act* (RISAA), em 19 de abril de 2024, renovando a autorização da secção 702 da FISA por um período de dois anos e introduzindo várias alterações. Estas podem genericamente dividir-se em duas categorias: 1) alterações no âmbito das atividades de vigilância permitidas ao abrigo da secção 702 da FISA e 2) alterações institucionais e processuais.

Alterações no âmbito das atividades de vigilância permitidas ao abrigo da secção 702 da FISA

A RISAA introduziu três alterações principais no âmbito das atividades de vigilância que podem ser realizadas ao abrigo da secção 702 da FISA.

Em primeiro lugar, a recolha de comunicações que contenham referências a um alvo, mas que não sejam desse alvo nem se destinem a ele (*abouts*), foi definitivamente proibida[47]. Trata-se da recolha de comunicações em que o seletor da secção 702 (como um endereço de correio eletrónico) não se encontra no campo «destinatário» ou «remetente» das comunicações, mas contém uma referência a esse seletor na comunicação (por exemplo, comunicações de correio eletrónico que não são enviadas para ou a partir do endereço de correio eletrónico selecionado, mas incluem o endereço de correio eletrónico selecionado no texto ou no corpo da mensagem de correio eletrónico). Embora essa recolha já tivesse sido excluída na sequência de uma alteração à FISA em 2018, a FISA ainda previa a possibilidade de reiniciar a recolha das tais «comunicações que contenham referências» no futuro, na sequência de um procedimento de autorização específico que envolvia o FISC e o Congresso. A última alteração introduzida pela RISAA eliminou esta possibilidade.

Em segundo lugar, a definição de informações externas foi alargada de modo a incluir informações relacionadas com o combate ao tráfico de droga[48]. Durante a reunião de avaliação, as autoridades dos EUA explicaram que tal foi introduzido à luz da atual crise do fentanilo e da crescente ameaça para a segurança nacional que os traficantes e fabricantes internacionais de estupefacientes representam. Neste contexto, foi confirmado que esta noção se enquadra em vários dos objetivos legítimos enumerados no EO 14086, ou seja, compreender ou avaliar as capacidades, intenções ou atividades de organizações estrangeiras que representam uma ameaça atual ou potencial para a segurança nacional dos EUA ou dos seus aliados; compreender ou avaliar as ameaças transnacionais com impacto na segurança mundial, incluindo os riscos para a saúde pública; e proteção contra ameaças criminosas transnacionais[49].

Em terceiro lugar, a RISAA ampliou a definição de «prestador de serviços de comunicações eletrónicas» , alargando assim o âmbito de empresas que podem ser obrigadas a fornecer informações nos termos da secção 702 da FISA[50]. A definição inclui agora outros prestadores de serviços que têm «acesso a equipamentos que estão a ser utilizados para transmitir ou

[46] https://www.intel.gov/foreign-intelligence-surveillance-act.
[47] Secção 22 da RISAA.
[48] Secção 23 da RISAA.
[49] Secção 2(b)(ii)(A)(2), (3) e (10) do EO 14086.
[50] Secção 25 da RISAA.

armazenar comunicações por fios ou eletrónicas ou podem servir para esse fim», excluindo explicitamente as unidades de alojamento públicas, as habitações, o equipamento público e os estabelecimentos de serviços de restauração. Numa carta ao Congresso, o DoJ referiu-se a esta alteração como uma alteração técnica destinada a abranger um número «extremamente pequeno» de empresas tecnológicas que, de acordo com as recentes decisões do FISC e do *Foreign Intelligence Surveillance Court of Review* (tribunal encarregado de apreciar os recursos relativos aos pedidos e mandatos em matéria de vigilância — FISCR), não estavam abrangidas pela anterior definição de prestador de serviços de comunicações eletrónicas[51]. Nessa mesma carta, o DoJ comprometeu-se a restringir o âmbito de aplicação, aplicando esta definição exclusivamente para abranger o tipo de prestador de serviços em causa no litígio que conduziu à decisão do FISC. Consequentemente, as empresas em causa são indicadas num anexo classificado destinado ao Congresso. Várias ONG, incluindo as que apresentaram observações no âmbito da avaliação, manifestaram preocupação em relação a esta expansão, alegando que poderia abranger muitas empresas dos EUA (uma vez que muitas delas prestam algum tipo de serviço e têm acesso a equipamento de comunicações). Tendo em conta essas preocupações, foi proposta uma nova alteração, com o apoio do setor das informações, num projeto de lei sobre a autorização de informações para o exercício fiscal de 2025, atualmente em apreciação no Congresso. Esta alteração, se aprovada pelo Congresso, assegurará que as empresas adicionais abrangidas pela definição de prestador de serviços de comunicações eletrónicas se limitarão apenas às mencionadas nos acórdãos do FISC acima referidos. O projeto de lei prevê igualmente que cada diretiva dirigida a essa empresa tenha de ser comunicada ao FISC, a fim de permitir que este verifique se a empresa seria efetivamente abrangida pelo âmbito de aplicação. Na sua carta ao Congresso, o DoJ comprometeu-se a apresentar-lhe, de seis em seis meses, um relatório sobre qualquer aplicação da definição atualizada, a fim de permitir ao Congresso exercer a supervisão adequada no que respeita à aplicação estrita da definição.

É importante salientar que, na reunião de avaliação, as autoridades dos EUA e a PCLOB confirmaram que todas as salvaguardas do EO 14086 continuam a ser plenamente aplicáveis a toda a recolha e utilização de dados ao abrigo da secção 702 da FISA, incluindo na sequência destas alterações. Assim, embora a RISAA alargue de certa forma o âmbito das empresas que podem receber um despacho, não limita o exercício dos direitos. No entanto, será importante continuar a acompanhar a evolução (legislativa e de apresentação de relatórios) e receber informações sobre a aplicação prática destas novas regras. Aqui se inclui, por exemplo, o impacto do alargamento das definições de informações externas e de prestador de serviços de comunicações eletrónicas no número de metas da secção 702 da FISA (conforme comunicado anualmente pelo ODNI, ver *infra* sobre a transparência). O futuro relatório de acompanhamento do recente relatório da PCLOB sobre a secção 702 do FISA (ver *infra*) deverá ser particularmente informativo a este respeito.

Questões institucionais e processuais

Em termos de alterações institucionais e processuais, a RISAA codificou vários procedimentos já seguidos na prática e introduziu novas salvaguardas. Embora algumas digam apenas respeito

[51] https://www.justice.gov/opa/media/1348621/dl?inline. Ver a decisão do FISC de 2022 (https://www.intel.gov/assets/documents/702%20Documents/declassified/2022-FISC-ECSP-OPINION.pdf) e o acórdão do *Foreign Intelligence Surveillance Court of Review* que confirma essa decisão (https://www.intel.gov/assets/documents/702%20Documents/declassified/2023_FISC-R_ECSP_Opinion.pdf).

a cidadãos dos EUA, várias alterações aumentam a proteção tanto de cidadãos dos EUA como de países terceiros cujos dados podem ser recolhidos ao abrigo da secção 702 da FISA[52] e são, por conseguinte, pertinentes para o funcionamento do QPD.

Em primeiro lugar, foram estabelecidos vários requisitos adicionais em matéria de responsabilização, supervisão e comunicação de informações. Em especial, o pessoal do FBI deve agora receber formação anual sobre as regras aplicáveis à consulta das informações obtidas ao abrigo da secção 702 da FISA[53]. O FBI é igualmente obrigado a informar o Congresso sobre as suas atividades de consulta (por exemplo, o número de consultas que utilizam «tecnologias de trabalho em lote», ou seja, a utilização de múltiplos termos de pesquisa como parte de uma única consulta) e sobre as medidas de responsabilização adotadas para assegurar o cumprimento dos requisitos legais de consulta (secções 11 e 12 da RISAA). Além disso, o inspetor-geral do DoJ é incumbido de elaborar um relatório sobre o cumprimento dos requisitos de consulta pelo FBI (secção 9 da RISAA). De um modo mais geral, para aumentar a transparência dos procedimentos perante o FISC, o ODNI e o Procurador-Geral são agora obrigados a concluir a reapreciação de desclassificação das decisões do FISC no prazo de 180 dias (secção 7 da RISAA). Além disso, as transcrições de todas as audiências perante o FISC e o *Foreign Intelligence Court of Review* (FISCR, em que as decisões do FISC podem ser objeto de recurso) devem ser conservadas e transmitidas ao Congresso (secção 8 da RISAA).

Em segundo lugar, a RISAA introduziu novas limitações à utilização pelo FBI dos dados recolhidos ao abrigo da secção 702 da FISA. A secção 2, alínea d), da RISAA prevê que uma consulta que utilize a «tecnologia em lotes» só pode ser efetuada após a obtenção da aprovação de um advogado dentro FBI, a menos que existam circunstâncias prementes. Além disso, o FBI está agora proibido de verificar automaticamente as informações não minimizadas obtidas ao abrigo da secção 702 da FISA e, em vez disso, é obrigado a assegurar que os analistas têm de selecionar afirmativamente a pesquisa dessas informações. A RISAA também proibiu o FBI de realizar consultas exclusivamente destinadas a encontrar e extrair provas de atividade criminosa (a menos que haja uma convicção razoável de que podem ajudar a atenuar ou eliminar uma ameaça à vida ou lesões corporais graves, ou quando necessário para cumprir as obrigações de divulgação em litígios)[54]. Além disso, o FBI está proibido de introduzir dados não minimizados em repositórios analíticos, a menos que a pessoa visada seja pertinente para uma investigação em curso em matéria de segurança nacional[55].

Em terceiro lugar, foram alteradas certas disposições relativas ao estatuto e ao papel de *amici curiae* perante o FISC[56]. Os *amici* são designados peritos para assistir o Tribunal (e o FISCR)

[52] Além disso, a RISAA introduziu algumas alterações no que diz respeito à vigilância eletrónica individualizada tradicional nos termos da secção 105 da FISA (com base num mandado do FISC emitido se o critério de causa provável estiver satisfeito). Um pedido apresentado por um serviço de informações ao Procurador-Geral para um despacho de realização de vigilância eletrónica individualizada exige agora uma declaração sob compromisso de honra que justifique a convicção de que as condições previstas na secção 105 da FISA estão preenchidas [secção 6, alínea a), da RISAA]. A possível duração da vigilância eletrónica no que respeita a potências ou agentes estrangeiros de potências estrangeiras foi alargada de 120 dias para um ano [secção 6, alínea g), da RISAA].

[53] Secção 2, alínea d), da RISAA.

[54] Secção 3, alínea a), da RISAA.

[55] Secção 3, alínea b), da RISAA. Sempre que necessário devido a circunstâncias prementes, o diretor do FBI pode decidir sobre uma exceção a esta disposição, que tem de ser notificada ao Congresso.

[56] Por razões de clareza, estas alterações não afetam o estatuto e o papel dos advogados especiais perante o *Data Protection Review Court* (DPRC), tal como confirmado pelos EUA na reunião de avaliação.

em questões relacionadas com a privacidade e as liberdades cívicas ou para ajudar a clarificar questões tecnológicas ao tratar de um pedido específico de um governo. Enquanto anteriormente a FISA exigia que os *amici* tivessem conhecimentos especializados em matéria de privacidade e liberdades cívicas, recolha de informações, tecnologias da comunicação ou outros domínios pertinentes, agora exige, em princípio, conhecimentos especializados em matéria de privacidade/liberdades cívicas e recolha de informações. O Tribunal já tinha a possibilidade de nomear um *amicus* em qualquer caso que considerasse adequado e estava obrigado a fazê-lo quando se trata de uma interpretação nova ou significativa da lei. Na sequência da renovação da autorização, o FISC é agora também obrigado a nomear uma *amicus* sempre que lhe for solicitado que aprove uma certificação prevista na secção 702 da FISA e procedimentos de acompanhamento (por exemplo, procedimentos de seleção de alvos), a menos que considere que tal não seria adequado ou provavelmente resultaria num atraso injustificado[57]. Além disso, em vez de nomear apenas um, o Tribunal pode agora decidir nomear um ou mais *amici*. Esclarece-se igualmente que as informações a fornecer por *amici* devem «limitar-se a abordar as questões específicas identificadas pelo Tribunal», embora os domínios sobre os quais o *amici* podem formular observações tenham permanecido amplos (ou seja, fundamentos jurídicos e informações relacionadas com a proteção da privacidade individual e das liberdades cívicas dos cidadãos dos Estados Unidos, recolha de informações e tecnologias da comunicação ou qualquer outro domínio relevante).

Por último, a secção 18 da RISAA cria uma «Comissão de Reforma da FISA» — composta, nomeadamente, por membros do Congresso, pelo presidente da PCLOB, pelo diretor adjunto principal do Serviço Nacional de Informações e pelo procurador-geral adjunto, bem como por membros adicionais a nomear pelo Congresso[58] — para recomendar reformas adicionais da FISA.

A Comissão acompanhará de perto a evolução da situação no que respeita à secção 702 da FISA, nomeadamente no contexto das atividades de supervisão da PCLOB (ver *infra*), do trabalho da Comissão de Reforma e da próxima avaliação da FISA após dois anos.

2.2.1.3. Atividades de vigilância na prática: números e tendências

O relatório anual do ODNI sobre a transparência estatística relativa à utilização, pelo setor das informações, das autoridades nacionais de vigilância da segurança para o ano civil de 2023 (publicado em abril de 2024)[59] mostra que o número de metas ao abrigo da secção 702 da FISA aumentou de 245 073 no ano civil de 2022 para 268 590 no ano civil de 2023. O relatório explica que as flutuações no número de metas podem estar associadas a várias razões, incluindo alterações nas prioridades operacionais, eventos mundiais, capacidades técnicas, comportamento dos alvos e mudanças no setor das telecomunicações. O relatório indica igualmente que não foram visados cidadãos de países terceiros (em comparação com 1 em 2021 e 0 em 2022) ao abrigo da secção 402 da FISA (dispositivos de registo de chamadas telefónicas e comunicações eletrónicas), ao passo que seis despachos (em comparação com 11 despachos tanto em 2021 como em 2022), para seis alvos (em comparação com 13 em 2021 e 11 em 2022), foram emitidos ao abrigo da secção 501 da FISA (acesso aos registos comerciais de empresas de transportes públicos, estabelecimentos de aluguer de veículos ou estabelecimentos físicos de armazenamento), abrangendo 5 412 identificadores únicos (em comparação com

[57] Secção 5, alínea b), da RISAA.
[58] A secção 18 exige especificamente a representação externa ao Congresso.
[59] https://www.dni.gov/files/CLPT/documents/2024_ASTR_for_CY2023.pdf.

23 157 em 2021 e 55 431 em 2022) utilizados para comunicar informações recolhidas nos termos desses despachos.

O relatório anual do DoJ relativo à *Foreign Intelligence Surveillance Act* (Lei de Vigilância de Informações Externas) apresentado ao Congresso indica que, durante o ano civil de 2023, foram apresentados 327 pedidos ao FISC para realizar vigilância eletrónica e/ou buscas físicas para efeitos de informações externas ao abrigo das secções 105 e 302 da FISA, respetivamente[60]. O número total de pessoas visadas situou-se entre 500 e 999. No que diz respeito às *National Security Letters* (cartas de segurança nacional — NSL), o relatório indica que foram emitidos 10 115 pedidos (excluindo apenas os pedidos de informações sobre assinantes) de informações sobre cidadãos de países terceiros, solicitando informações relativas a 3 033 cidadãos de países terceiros diferentes[61].

Várias empresas certificadas no âmbito do QPD (por exemplo, a Google e a Meta) recorrem à possibilidade prevista na legislação dos EUA de publicar relatórios de transparência que informam sobre o número de pedidos da FISA e de NSL que receberam durante um determinado período de referência. À data da elaboração do presente relatório, as estatísticas sobre os pedidos da FISA após julho de 2023 ainda não estavam disponíveis. A Google, por exemplo, comunicou ter recebido entre 500 e 999 pedidos de NSL, afetando entre 2 000 e 2 499 contas, entre julho e dezembro de 2023[62]. A Meta comunicou que recebeu entre 0 e 499 pedidos de NSL, afetando 500 a 999 contas, no mesmo período de referência[63]. Os números mantiveram-se bastante estáveis nos últimos anos. Para aumentar ainda mais a transparência, algumas empresas (por exemplo, a Google) publicam proativamente a NSL que receberam assim que as restrições de não divulgação são levantadas[64].

2.2.1.4. Outros desenvolvimentos

No contexto da preparação da avaliação, várias ONG levantaram questões sobre novas formas de obtenção de dados pelos serviços de informações dos EUA através da aquisição de dados a entidades comerciais, em especial corretores de dados. Explicaram que, embora os dados recolhidos nesta base devam continuar a ser tratados em conformidade com outros requisitos, incluindo, por exemplo, ao abrigo do EO 12333[65], essa obtenção tem lugar fora do enquadramento da FISA e do EO 14086.

A este respeito, importa recordar que qualquer tipo de partilha voluntária de dados com terceiros está sujeita a várias condições pormenorizadas no âmbito do QPD. Em primeiro lugar, a organização certificada não pode partilhar dados com um terceiro (que não atue na qualidade de agente/subcontratante) sem aplicar os princípios de aviso e escolha aos cidadãos em causa[66]. Em segundo lugar, em conformidade com o *princípio de responsabilização pela transferência*

[60] https://www.justice.gov/nsd/media/1350236/dl?inline.
[61] Estes valores mantiveram-se, em grande medida, estáveis em comparação com o ano de referência anterior (2022). Em comparação, em 2022, houve 317 pedidos finais ao FISC para efetuar vigilância eletrónica e/ou buscas físicas para efeitos de informações externas. O número total de pessoas visadas por despachos de vigilância eletrónica situou-se entre 0 e 499. Em 2022, o FBI apresentou 9 103 pedidos de NSL para informações sobre cidadãos de países terceiros (excluindo apenas os pedidos de informações sobre assinantes). Fonte: https://irp.fas.org/agency/doj/fisa/2022rept.pdf.
[62] https://transparencyreport.google.com/user-data/us-national-security.
[63] https://transparency.meta.com/reports/government-data-requests/country/US/.
[64] https://transparencyreport.google.com/user-data/us-national-security.
[65] Ver, por exemplo, secção 2.4 do EO 12333 sobre técnicas de recolha.
[66] Ver considerando 40 da decisão de adequação.

ulterior, as transferências ulteriores só podem ser efetuadas 1) para finalidades limitadas e específicas, 2) com base num contrato entre a organização do QPD UE-EUA e o terceiro e 3) se esse contrato exigir unicamente que o terceiro assegure o mesmo nível de proteção que o garantido pelos princípios[67].

Além disso, tal como também foi debatido durante a reunião de avaliação, a FTC tomou medidas coercivas contra os corretores de dados que vendem dados sensíveis dos consumidores. Por exemplo, num processo contra a X-Mode e a sua sucessora Outlogic, a FTC adotou, em 9 de janeiro de 2024, um despacho que proibia a empresa de vender dados de geolocalização a terceiros e de apagar os dados que tinha utilizado e partilhado ilegalmente. A investigação da FTC revelou, nomeadamente, que a empresa não informou plenamente os cidadãos sobre a utilização e a venda dos seus dados de geolocalização, não pôs em prática medidas que permitissem a autoexclusão do rastreio, permitiu a utilização dos dados para fins potencialmente discriminatórios e não limitou a utilização dessas informações por terceiros[68]. A Comissão espera que a FTC adote a mesma abordagem se as empresas certificadas no âmbito do QPD partilharem dados em violação das disposições acima referidas.

Por último, importa referir que, em maio de 2024, o ODNI publicou o*Intelligence Community Policy Framework for Commercially Available Information*[69]. Este quadro estabelece uma série de princípios e requisitos que os serviços de informações devem respeitar, nomeadamente para minimizar os riscos para a privacidade e as liberdades cívicas, aquando da obtenção e utilização de informações no contexto de uma transação comercial.

2.2.2. Supervisão independente

As atividades dos serviços de informações dos EUA estão sujeitas à supervisão de diferentes organismos, incluindo os agentes responsáveis pela proteção da privacidade e das liberdades cívicas, os inspetores-gerais, o Congresso e a PCLOB. Em especial, o EO 14086 exige que cada serviço de informações tenha funcionários a nível superior com experiência nos domínios jurídico, da supervisão e da conformidade para assegurar o cumprimento da legislação dos EUA aplicável. Esta função de supervisão é desempenhada por agentes com uma função de verificação da conformidade designada, bem como por agentes responsáveis pela proteção da privacidade e das liberdades cívicas e por inspetores-gerais[70]. Os referidos funcionários devem efetuar uma supervisão periódica das atividades de informação de origem eletromagnética e assegurar a correção de qualquer incumprimento identificado. Os serviços de informações

[67] Ver considerando 38 da decisão de adequação.

[68] https://www.ftc.gov/news-events/news/press-releases/2024/01/ftc-order-prohibits-data-broker-x-mode-social-outlogic-selling-sensitive-location-data.

[69] https://www.dni.gov/files/ODNI/documents/CAI/Commercially-Available-Information-Framework-May2024.pdf. Os serviços de informações têm de cumprir o quadro desde agosto de 2024.

[70] Cada serviço de informações dispõe de um inspetor-geral juridicamente independente e responsável pela realização de auditorias e investigações relacionadas com as atividades exercidas pelo respetivo serviço para efeitos de segurança nacional. Têm acesso a todos os materiais pertinentes (incluindo o material classificado), através de intimações, se necessário, e podem recolher depoimentos. Os inspetores-gerais remetem os casos de suspeita de infrações penais para os tribunais para o exercício da ação penal e formulam recomendações sobre medidas corretivas destinadas aos diretores dos serviços. Embora as suas recomendações não sejam vinculativas, os seus relatórios, incluindo sobre as medidas de acompanhamento (ou a sua inexistência), são geralmente tornados públicos e transmitidos ao Congresso. Ver, a este respeito, a nota de rodapé 136 da decisão de adequação sobre o papel do inspetor-geral.

devem fornecer a esses funcionários acesso a todas as informações relevantes para o exercício das suas funções de supervisão e não podem tomar quaisquer medidas para impedir ou influenciar indevidamente as suas atividades de supervisão.

O conselheiro-geral do *Office of the Intelligence Community Inspector General* (ICIG) no ODNI — que tem ampla competência sobre todo o setor das informações e está autorizado a investigar queixas ou informações relativas a alegações de conduta ilícita ou abuso de autoridade — participou na reunião de avaliação. Confirmou que o ICIG verifica sistematicamente o cumprimento do EO 14086 enquanto parte das suas atividades de supervisão. Referiu igualmente as recentes atividades de supervisão de outros inspetores-gerais do setor das informações, tal como descrito em relatórios periódicos. Por exemplo, no seu relatório semestral ao Congresso relativo a abril-setembro de 2023[71], o inspetor-geral da NSA prestou informações sobre uma avaliação de um quadro de controlo interno da NSA para decisões e pedidos de seleção de alvos. Concluiu afirmando que este quadro funcionava corretamente para garantir o cumprimento das leis, diretivas e políticas que protegem as liberdades cívicas e a privacidade. O mesmo relatório menciona igualmente uma investigação que revelou a utilização abusiva, por parte de um funcionário da NSA, de uma ferramenta de informação de origem eletromagnética para fins não autorizados.

No âmbito do EO 14086, são confiadas à PCLOB[72] funções de supervisão específicas[73]. A presidente da PCLOB e os seus três membros participaram na reunião de avaliação e informaram que a PCLOB prestou aconselhamento aos serviços de informações sobre os seus projetos de políticas e procedimentos de execução do EO 14086 em abril de 2023, tendo sido consultada sobre a nomeação de juízes e advogados especiais do *Data Protection Review Court* (DPRC). A PCLOB lançou igualmente um projeto de supervisão para 1) avaliar a aplicação das políticas e procedimentos atualizados adotados pelos serviços de informações, a fim de assegurar a sua coerência com o OE, e 2) realizar uma avaliação anual do funcionamento do novo mecanismo de recurso (ver *infra*)[74]. Os membros da PCLOB confirmaram que esta tenciona realizar ambas as avaliações num futuro próximo. No que respeita ao recurso, explicaram que, na ausência de queixas, a avaliação da PCLOB centrar-se-á nas políticas e procedimentos estabelecidos para criar o mecanismo.

Em termos de outras atividades de supervisão, a PCLOB publicou um relatório sobre a secção 702 da FISA em 28 de setembro de 2023[75]. O referido relatório dá seguimento a um relatório anterior de 2014 e contém informações factuais e jurídicas atualizadas sobre o funcionamento

[71] https://oig.nsa.gov/reports/Article/3609957/semiannual-report-to-congress-1-april-2023-to-30-september-2023/.

[72] A PCLOB é uma agência independente com responsabilidades no domínio das políticas de luta contra o terrorismo e da sua aplicação, com vista à proteção da privacidade e das liberdades cívicas. Pode aceder a todas as informações pertinentes (incluindo informações classificadas), realizar entrevistas e recolher depoimentos. Pode formular recomendações às autoridades responsáveis pela aplicação da lei e aos serviços de informações e informar regularmente o Congresso e o presidente. Os seus relatórios são, tanto quanto possível, disponibilizados ao público.

[73] https://documents.pclob.gov/prod/Documents/EventsAndPress/834a1977-f420-4b2a-ae93-8a522b2c7c74/Trans-Atlantic%20Data%20Privacy%20Framework%20EO%20press%20release%20(FINAL)%20-%20Completed%20508%20-%2010202022.pdf.

[74] https://www.pclob.gov/OversightProjects/Details/1115.

[75] https://documents.pclob.gov/prod/Documents/OversightReport/8ca320e5-01d3-4d6a-8106-3384aad6ff31/2023%20PCLOB%20702%20Report%20-%20Nov%2017%202023%20-%201446.pdf.

dos programas de vigilância da secção 702 da FISA. O relatório contém igualmente recomendações sobre o cumprimento, por parte dos serviços de informações, dos requisitos aplicáveis e sugestões ao Congresso para reforçar vários aspetos da secção 702 da FISA no contexto da sua renovação da autorização (nomeadamente codificando os objetivos legítimos das atividades de vigilância enumerados no EO 14086)[76]. Durante a reunião de avaliação, a PCLOB informou que espera receber a breve trecho respostas dos serviços de informações sobre a aplicação das suas recomendações, que serão tidas em conta num futuro relatório de acompanhamento. Outros projetos de supervisão em curso incluem um sobre a luta contra o terrorismo interno e o seu impacto na privacidade e nas liberdades cívicas e a recolha de dados de fonte aberta ou comercialmente disponíveis pelo FBI[77].

Por último, ONG consultadas no contexto da avaliação manifestaram preocupação em relação ao facto de o mandato de vários membros da PCLOB expirar em breve, podendo deixar a PCLOB sem quórum. Em especial, o mandato da presidente expirou e o período durante o qual pode exercer funções a título interino termina em janeiro de 2025, enquanto outro lugar está vago e um terceiro cessará também em janeiro do próximo ano. Durante a reunião de avaliação, os membros explicaram que não preveem que a PCLOB fique sem quórum, uma vez que já foi emitida uma nomeação para o lugar atualmente vago (aguardando confirmação do Senado)[78]. Sublinharam igualmente que, mesmo que a PCLOB ficasse sem quórum, tal não afetaria a sua capacidade para continuar a realizar projetos de supervisão. No entanto, dado o papel importante que a PCLOB desempenha na avaliação da execução do EO 14086, a Comissão acompanhará de perto a situação das futuras vagas e designações/nomeações.

2.2.3. Recurso

O EO 14086, complementado por um regulamento do Procurador-Geral, criou um novo mecanismo de recurso para tratar e resolver queixas admissíveis de cidadãos relativas a atividades de informação de origem eletromagnética dos EUA[79]. Qualquer cidadão na UE tem o direito de apresentar uma queixa ao mecanismo de recurso relativamente a uma alegada violação da legislação dos EUA que rege as atividades de informação de origem eletromagnética (por exemplo, o EO 14086, a secção 702 da FISA, o EO 12333), no que respeita a dados pessoais transferidos para os EUA que afetem negativamente os seus interesses em matéria de privacidade e liberdades cívicas. Os cidadãos podem apresentar uma queixa a uma APD num Estado-Membro da UE, que a reencaminha, através do secretariado do CEPD, para o mecanismo de recurso. O mecanismo consiste em dois níveis, com a investigação inicial das queixas realizada pelo CLPO do ODNI e a possibilidade de os cidadãos recorrerem da decisão do CLPO junto de um DPRC independente. Uma vez concluída a análise pelo CLPO do ODNI ou pelo DPRC, os cidadãos são informados, através da autoridade nacional, de que «a análise não identificou quaisquer violações abrangidas ou o CLPO do ODNI/DPRC emitiu uma decisão que exige a aplicação de medidas corretivas adequadas». As decisões do CLPO do ODNI e do DPRC são vinculativas para os serviços de informações.

---

[76] A Comissão observa que algumas dessas recomendações foram incorporadas como parte da RISAA, designadamente a recomendação sobre a recolha de comunicações que contenham referências ou a recomendação sobre o reforço do papel dos peritos do FISC (*amici*).

[77] https://www.pclob.gov/OversightProjects.

[78] https://documents.pclob.gov/prod/Documents/EventsAndPress/deb9cd13-12af-4250-998e-a520a2419a6b/PCLOB%20nominee%20press%20release%206-13-24.pdf.

[79] Considerandos 176 a 194 da decisão de adequação.

Desde a adoção da decisão de adequação, foram tomadas novas medidas para tornar o mecanismo de recurso plenamente operacional.

No que respeita à criação do DPRC, foram nomeados para o tribunal, em 14 de novembro de 2023, oito juízes [ou seja, mais dois do que o número mínimo exigido ao abrigo do EO 14086, complementado pela regulamentação do Procurador-Geral no título 28 do C.F.R. § 201.3(a)][80]. Foram nomeados com base nos critérios estabelecidos no EO 14086 e em conformidade com o processo nele estabelecido, incluindo após consulta, nomeadamente, da PCLOB[81]. Incluem antigos juízes dos tribunais federais distritais e do Tribunal de Recurso, um antigo Procurador-Geral dos EUA e um antigo membro da PCLOB. Conforme exigido pelo EO, pelo menos metade dos juízes tem experiência judicial anterior. Além disso, em abril de 2024, foram nomeados dois advogados especiais — profissionais da justiça com conhecimentos especializados tanto em matéria de privacidade como de segurança nacional — para representar os interesses dos cidadãos perante o DPRC. Foi confirmado na reunião de avaliação que todos os juízes e advogados especiais receberam a mais elevada credenciação de segurança e, por conseguinte, podem ter acesso a materiais classificados no desempenho das suas funções para o DPRC. O DPRC publicou igualmente uma série de perguntas frequentes, fornecendo mais informações sobre a sua função, independência e funcionamento[82].

No que respeita ao tratamento de queixas, o ODNI adotou, em 6 de dezembro de 2022, a *Intelligence Community Directive 126*, que regula em pormenor (estabelecendo prazos, criando um repositório eletrónico seguro e canais de comunicação, exigindo que os elementos do CLPO e do setor das informações cooperem com a PCLOB no contexto da avaliação anual do mecanismo de recurso, etc.) diferentes aspetos do processo de investigação e decisão das queixas[83]. A diretiva é aplicável em todo o setor das informações dos EUA e foi complementada por outros procedimentos internos, adotados por serviços de informações individuais sobre a sua cooperação com o CLPO do ODNI no contexto do tratamento de uma queixa (por exemplo, elaboração de um repositório seguro para a partilha de queixas e documentos de resposta; e comunicações seguras entre os serviços competentes). Nos próximos meses, o DPRC emitirá igualmente regras mais pormenorizadas sobre o tratamento das queixas e outros aspetos processuais.

Foram tomadas várias medidas adicionais na União Europeia e nos Estados Unidos para informar o público em geral, bem como para facilitar a apresentação e o tratamento de queixas. Tal inclui a adoção pelo CEPD de uma nota informativa sobre o novo mecanismo de recurso[84], um modelo de formulário de apresentação de queixas (que deverá ser traduzido e publicado por todas as APD nas suas línguas nacionais)[85] e o regulamento interno que rege a cooperação entre as autoridades nacionais de controlo e o secretariado do CEPD[86]. Do mesmo modo, o

[80] https://www.justice.gov/opa/pr/attorney-general-merrick-b-garland-announces-judges-data-protection-review-court.
[81] Secção 3(d)(A) do EO 14086.
[82] https://www.justice.gov/opcl/dprc-resources.
[83] https://www.dni.gov/files/documents/ICD/ICD_126-Implementation-Procedures-for-SIGINT-Redress-Mechanism.pdf.
[84] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/information-note-data-protection-framework-redress_pt.
[85] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/template-complaint-form-us-office-director-national_pt.
[86] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/rules-procedure-data-protection-framework-redress_pt.

ODNI publicou perguntas frequentes e uma ficha informativa sobre o novo mecanismo de recurso e participou em atividades de sensibilização do público[87].

Além disso, ao longo do último ano, o CEPD e as autoridades competentes dos EUA cooperaram estreitamente em vários aspetos operacionais. Em especial, tal como confirmado durante a reunião de avaliação, criaram um canal de comunicação cifrado para transmitir queixas das autoridades nacionais da UE ao secretariado do CEPD, do secretariado do CEPD ao CLPO do ODNI, bem como ao *Office of Privacy and Civil Liberties* (OPCL) do DoJ, e entre o CLPO do ODNI e outras autoridades do lado dos EUA (por exemplo, o DPRC). Além disso, o CLPO do ODNI explicou que foram criados outros procedimentos internos para a cooperação de serviços de informações individuais com o CLPO do ODNI, no que se refere ao tratamento de queixas.

Por último, o OPCL, que presta apoio administrativo ao DPRC, informou igualmente que o DPRC opera ao abrigo da sua própria rubrica orçamental específica e dispõe dos equipamentos necessários para desempenhar as suas funções, incluindo computadores de mesa e computadores portáteis seguros, telefones, etc. Além disso, tal como exigido pelo EO 14086, o DoC tomou as medidas necessárias, nomeadamente através da criação de um canal de comunicação cifrado com o CLPO do ODNI, a fim de manter um registo de todas as queixas admissíveis recebidas. O DoC contactará periodicamente o CLPO do ODNI para determinar se as informações relativas a uma queixa individual foram desclassificadas. Em caso afirmativo, o DoC notificará do facto o cidadão em causa, a fim de lhe permitir obter acesso a essas informações.

À data da reunião de avaliação, as autoridades de controlo da UE não tinham recebido queixas, pelo que o novo mecanismo de recurso ainda não tinha sido acionado.

3. CONCLUSÃO

Com base nas informações recolhidas durante esta primeira avaliação, a Comissão conclui que as autoridades dos EUA criaram as estruturas e os procedimentos necessários para assegurar o funcionamento eficaz do Quadro de Privacidade de Dados. Neste contexto, a Comissão valoriza vivamente a cooperação muito positiva com as autoridades dos EUA na realização da avaliação.

Embora esta primeira avaliação se tenha naturalmente centrado na verificação da existência de todos os elementos constitutivos do quadro, a experiência com a aplicação prática das salvaguardas aplicáveis tanto ao tratamento de dados por empresas certificadas como ao acesso aos dados por parte das autoridades públicas é necessariamente limitada, decorrido apenas um ano de funcionamento. Por conseguinte, a Comissão acompanhará de perto os desenvolvimentos pertinentes nos próximos meses e anos, prestando especial atenção 1) aos próximos relatórios da PCLOB sobre a aplicação do EO 14086 e o funcionamento do mecanismo de recurso em matéria de informações de origem eletromagnética, em especial no que diz respeito ao DPRC; 2) a eventuais novas alterações da secção 702 da FISA; e 3) à designação e nomeação de membros da PCLOB para preencher as próximas vagas.

[87] https://www.dni.gov/files/CLPT/documents/Fact_Sheets/The_Role_of_the_ODNI_CLPO_FAQs.pdf e https://www.dni.gov/files/CLPT/documents/Fact_Sheets/Data_Privacy_Framework.pdf.

Além disso, a fim de assegurar um funcionamento contínuo e eficaz, a Comissão considera importante que:

- como anunciado na reunião de avaliação, o DoC utilize plenamente os diferentes instrumentos previstos no QPD para o controlo do cumprimento dos princípios por parte das empresas e a deteção de falsas alegações de participação,
- a FTC desenvolva ainda mais a sua abordagem proativa em matéria de investigação e execução do cumprimento dos princípios do QPD por parte das empresas certificadas e
- o DoC, a FTC e as autoridades de proteção de dados da UE criem instrumentos de orientação comuns sobre os principais requisitos no âmbito dos princípios do QPD, por exemplo, sobre dados de recursos humanos e transferências ulteriores.

Tendo em conta este resultado da avaliação e tal como previsto no considerando 211 da decisão de adequação, a Comissão considera apropriado realizar a próxima avaliação periódica após três anos. Este período deverá permitir adquirir mais experiência com a aplicação prática do QPD e ter em conta os desenvolvimentos futuros acima referidos. Por conseguinte, em conformidade com o artigo 3.º, n.º 4, da decisão de adequação, a Comissão consultará o CEPD e o comité criado nos termos do artigo 93.º, n.º 1, do Regulamento Geral sobre a Proteção de Dados relativamente à periodicidade das futuras avaliações.