Conselho da
União Europeia

Bruxelas, 22 de janeiro de 2024
(OR. en)

5454/24

DATAPROTECT 23
JAI 62
RELEX 42

NOTA DE ENVIO

de:	Secretária-geral da Comissão Europeia, com a assinatura de Martine DEPREZ, diretora
para:	Thérèse BLANCHET, secretária-geral do Conselho da União Europeia
n.° doc. Com.:	COM(2024) 7 final
Assunto:	RELATÓRIO DA COMISSÃO AO PARLAMENTO EUROPEU E AO CONSELHO sobre a primeira revisão do funcionamento das decisões de adequação adotadas nos termos do artigo 25.º, n.º 6, da Diretiva 95/46/CE

Envia-se em anexo, à atenção das delegações, o documento COM(2024) 7 final.

Anexo: COM(2024) 7 final

COMISSÃO
EUROPEIA

Bruxelas, 15.1.2024
COM(2024) 7 final

RELATÓRIO DA COMISSÃO AO PARLAMENTO EUROPEU E AO CONSELHO

sobre a primeira revisão do funcionamento das decisões de adequação adotadas nos termos do artigo 25.º, n.º 6, da Diretiva 95/46/CE

{SWD(2024) 3 final}

1. PRIMEIRA REVISÃO — ANTECEDENTES E CONTEXTO

O presente relatório contém as conclusões da Comissão sobre a primeira revisão das decisões de adequação adotadas com base no artigo 25.º, n.º 6, da Diretiva 95/46/CE[1] (Diretiva Proteção de Dados).

Nessas decisões, a Comissão determinou que 11 países ou territórios asseguram um nível adequado de proteção dos dados pessoais transferidos da União Europeia (UE)[2]: Andorra[3], Argentina[4], Canadá (para os operadores comerciais)[5], Ilhas Faroé[6], Guernesey[7], Ilha de Man[8], Israel[9], Jersey[10], Nova Zelândia[11], Suíça[12] e Uruguai[13]. Consequentemente, as transferências de dados da UE para esses países ou territórios podem ser efetuadas sem exigências adicionais.

Com o início da aplicação do Regulamento (UE) 2016/679[14] (RGPD), em 25 de maio de 2018, as decisões de adequação adotadas ao abrigo da Diretiva Proteção de Dados permaneceram em

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

[2] Após a sua integração no Acordo sobre o Espaço Económico Europeu (EEE), o Regulamento Geral sobre a Proteção de Dados (RGPD) também se aplica à Noruega, à Islândia e ao Listenstaine. As referências à UE no presente relatório devem ser entendidas como abrangendo também os Estados do EEE.

[3] Decisão 2010/625/UE da Comissão, de 19 de outubro de 2010, nos termos da Diretiva 95/46/CE do Parlamento Europeu e do Conselho relativa à adequação do nível de proteção de dados pessoais em Andorra (JO L 277 de 21.10.2010, p. 27).

[4] Decisão 2003/490/CE da Comissão, de 30 de junho de 2003, nos termos da Diretiva 95/46/CE do Parlamento Europeu e do Conselho relativa à adequação do nível de proteção de dados pessoais na Argentina (JO L 168 de 5.7.2003, p. 19).

[5] Decisão 2002/2/CE da Comissão, de 20 de dezembro de 2001, nos termos da Diretiva 95/46/CE do Parlamento Europeu e do Conselho relativa à adequação do nível de proteção proporcionado pela lei canadiana sobre dados pessoais e documentos eletrónicos (Personal Information and Electronic Documents Act) (JO L 2 de 4.1.2002, p. 13).

[6] Decisão 2010/146/UE da Comissão, de 5 de março de 2010, nos termos da Diretiva 95/46/CE do Parlamento Europeu e do Conselho relativamente à adequação do nível de proteção assegurado pela Lei sobre o tratamento de dados pessoais das Ilhas Faroé (JO L 58 de 9.3.2010, p. 17).

[7] Decisão 2003/821/CE da Comissão, de 21 de novembro de 2003, relativa à adequação do nível de proteção de dados pessoais em Guernsey (JO L 308 de 25.11.2003, p. 27).

[8] Decisão 2004/411/CE da Comissão, de 28 de abril de 2004, relativa à adequação do nível de proteção de dados pessoais na Ilha de Man (JO L 151 de 30.4.2004, p. 48).

[9] Decisão 2011/61/UE da Comissão, de 31 de janeiro de 2011, nos termos da Diretiva 95/46/CE do Parlamento Europeu e do Conselho relativa à adequação do nível de proteção de dados pessoais pelo Estado de Israel no que se refere ao tratamento automatizado de dados (JO L 27 de 1.2.2011, p. 39).

[10] Decisão 2008/393/CE da Comissão, de 8 de maio de 2008, nos termos da Diretiva 95/46/CE do Parlamento Europeu e do Conselho relativa à adequação do nível de proteção de dados pessoais em Jersey (JO L 138 de 28.5.2008, p. 21).

[11] Decisão de Execução 2013/65/UE da Comissão, de 19 de dezembro de 2012, nos termos da Diretiva 95/46/CE do Parlamento Europeu e do Conselho relativa à adequação do nível de proteção de dados pessoais pela Nova Zelândia (JO L 28 de 30.1.2013, p. 12).

[12] Decisão 2000/518/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 adequado dos dados pessoais na Suíça (JO L 215 de 25.8.2000, p. 1).

[13] Decisão de Execução 2012/484/UE da Comissão, de 21 de agosto de 2012, nos termos da Diretiva 95/46/CE do Parlamento Europeu e do Conselho relativa à adequação do nível de proteção de dados pessoais pela República Oriental do Uruguai no que se refere ao tratamento automatizado de dados (JO L 227 de 23.8.2012, p. 11).

[14] 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).

vigor[15]. Simultaneamente, o RGPD clarificou que as conclusões de adequação são «instrumentos vivos», estipulando que a Comissão tem de controlar, de forma continuada, os desenvolvimentos nos países terceiros que possam afetar o funcionamento das decisões de adequação em vigor[16]. Além disso, o artigo 97.º do RGPD exige que a Comissão reveja periodicamente estas decisões, de quatro em quatro anos, a fim de determinar se os países e territórios objeto de uma conclusão de adequação continuam a proporcionar um nível adequado de proteção dos dados pessoais.

Esta primeira revisão das decisões de adequação adotadas ao abrigo do anterior quadro de proteção de dados da UE foi iniciada no âmbito de uma avaliação mais ampla da aplicação e do funcionamento do RGPD, sobre a qual a Comissão apresentou as suas conclusões na Comunicação intitulada «A proteção de dados enquanto pilar da capacitação dos cidadãos e a abordagem da UE para a transição digital — dois anos de aplicação do Regulamento Geral sobre a Proteção de Dados»[17]. No entanto, a conclusão deste aspeto da revisão foi adiada a fim de ter em conta o acórdão do Tribunal de Justiça no processo Schrems II[18], no qual o Tribunal de Justiça forneceu esclarecimentos importantes sobre elementos fundamentais do padrão de adequação, bem como outros desenvolvimentos conexos. Por sua vez, tal conduziu a intercâmbios aprofundados com os países e territórios em causa sobre aspetos pertinentes do seu quadro jurídico, mecanismos de supervisão e sistema de execução[19]. O presente relatório tem plenamente em conta todos estes desenvolvimentos, tanto na UE como nos países e territórios terceiros em causa.

Importa salientar que esta primeira revisão tem lugar no contexto do desenvolvimento exponencial das tecnologias digitais. Nas últimas décadas, a importância das decisões de adequação aumentou consideravelmente, à medida que os fluxos de dados se tornaram parte integrante da transformação digital da sociedade e da globalização da economia. A transferência de dados além-fronteiras passou a fazer parte das operações diárias das empresas europeias de todas as dimensões e em todos os setores. Mais do que nunca, o respeito da privacidade é uma condição para fluxos comerciais estáveis, seguros e competitivos. Neste contexto, as decisões de adequação desempenham um papel cada vez mais importante em muitos aspetos. Ao assegurarem que a proteção acompanha os dados, permitem fluxos de dados seguros, respeitando os direitos das pessoas, em consonância com a abordagem da transformação digital da UE centrada no ser humano. Ao envolverem o reconhecimento de um quadro de privacidade

[15] Ver artigo 45.º, n.º 9, do RGPD, que prevê que as decisões adotadas pela Comissão com base no artigo 25.º, n.º 6, da Diretiva 95/46/CE permanecem em vigor até que sejam alteradas, substituídas ou revogadas por uma decisão da Comissão adotada em conformidade com o n.º 3 ou o n.º 5 do artigo 45.º.
[16] Artigo 45.º, n.º 4, do RGPD. Ver também acórdão do Tribunal de Justiça da União Europeia de 6 de outubro de 2015, Maximillian Schrems/Data Protection Commissioner (Schrems I), C-362/14, ECLI:EU:C:2015:650, n.º 76.
[17] A comunicação foi publicada em junho de 2020 e está disponível na seguinte ligação: https://ec.europa.eu/info/law/law-topic/data-protection/communication-two-years-application-general-data-protection-regulation_en.
[18] Acórdão do Tribunal de Justiça da União Europeia de 16 de julho de 2020, Data Protection Commissioner/Facebook Ireland Ltd e Maximillian Schrems (Schrems II), C-311/18, ECLI:EU:C:2020:559.
[19] A decisão de adequação relativa ao Japão foi adotada com base no RGPD e prevê uma revisão periódica distinta. A primeira revisão foi concluída em abril de 2023 com o Relatório da Comissão ao Parlamento Europeu e ao Conselho sobre a primeira avaliação da aplicação da decisão de adequação relativa ao Japão, COM(2023) 275 final, disponível na seguinte ligação: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=COM:2023:275:FIN.

de países terceiros como proporcionando um nível de proteção essencialmente equivalente ao da UE, promovem a convergência entre os sistemas de privacidade baseados em elevados padrões de proteção. Além disso, como se explica no presente relatório, em vez de serem um «ponto final», as decisões de adequação lançaram as bases para uma cooperação mais estreita e uma maior convergência regulamentar entre a UE e parceiros que partilham a mesma visão. Ao permitirem a livre circulação de dados pessoais, estas decisões abriram canais comerciais aos operadores da UE, nomeadamente completando e ampliando os benefícios dos acordos comerciais, tendo facilitado a cooperação com parceiros estrangeiros num vasto leque de domínios regulamentares. Ao proporcionarem uma solução simples e abrangente para as transferências de dados sem necessidade de o exportador de dados apresentar garantias adicionais ou obter qualquer autorização, facilitam o cumprimento, em especial por parte das pequenas e médias empresas, dos requisitos de transferência internacionais do RGPD. Por último, graças ao seu «efeito de rede», as decisões de adequação adotadas pela Comissão Europeia são cada vez mais pertinentes também fora da UE, uma vez que permitem não só a livre circulação de dados com as 30 economias da UE, mas também com muitas mais jurisdições em todo o mundo[20] que reconhecem os países para os quais existe uma decisão de adequação da UE como «destinos seguros» ao abrigo das suas próprias regras de proteção de dados.

Por todas estas razões, como também confirmado pelo diálogo intenso e frutuoso com os países/territórios terceiros em causa subjacente à revisão em questão, as decisões de adequação tornaram-se uma componente estratégica da relação global da UE com estes parceiros estrangeiros e são reconhecidas como um dos principais facilitadores do aprofundamento da cooperação num vasto leque de domínios. Por conseguinte, é particularmente importante que estas decisões possam resistir ao teste do tempo e dar resposta a novos desenvolvimentos e desafios.

2. OBJETO E METODOLOGIA DA REVISÃO

As decisões de adequação que são objeto da revisão em causa foram adotadas ao abrigo do quadro de proteção de dados da UE que precedeu o RGPD. Embora as decisões mais recentes datem de há cerca de uma década (por exemplo, as decisões relativas à Nova Zelândia e ao Uruguai, ambas adotadas em 2012), outras estão em vigor há mais de vinte anos (por exemplo, a relativa ao Canadá, adotada em 2001, e a relativa à Suíça, adotada em 2000). Desde então, os quadros de proteção de dados nos 11 países e territórios evoluíram, por exemplo, através de reformas legislativas ou regulamentares, da evolução da prática de execução das autoridades de proteção de dados ou da jurisprudência.

Ao realizar a sua avaliação, a Comissão centrou-se, por conseguinte, na evolução dos quadros de proteção de dados dos países e territórios pertinentes desde a adoção da decisão de adequação, tendo avaliado a forma como esta evolução moldou ainda mais o panorama da proteção de dados do país ou território pertinente e se, tendo em conta esta evolução, os vários regimes continuam a assegurar um nível de proteção adequado.

[20] Por exemplo, Argentina, Colômbia, Israel, Marrocos, Suíça e Uruguai.

Para o efeito, teve-se plenamente em conta a evolução do próprio regime de proteção de dados da UE, em especial com o início da aplicação do RGPD. Em especial, desde a adoção destas decisões de adequação, a norma jurídica aplicável a tais decisões, bem como os elementos pertinentes para avaliar se um sistema estrangeiro assegura um nível de proteção adequado, foram clarificados através da jurisprudência do Tribunal de Justiça e das orientações adotadas pelo Grupo de Trabalho do artigo 29.º e pelo seu sucessor, o Comité Europeu para a Proteção de Dados[21] (CEPD).

Nomeadamente, o Tribunal de Justiça, no seu acórdão de 6 de outubro de 2015 no processo Schrems I, estabeleceu que, embora não se possa exigir que um país terceiro assegure um nível de proteção idêntico ao garantido na UE, o teste de adequação deve ser entendido no sentido de que exige um nível de proteção «substancialmente equivalente»[22]. Em especial, o Tribunal de Justiça esclareceu que os meios a que o país terceiro em causa recorre para proteger os dados pessoais podem ser diferentes dos implementados na União, desde que se revelem, na prática, eficazes para assegurar um nível de proteção adequado[23]. Por conseguinte, o teste de adequação exige uma avaliação exaustiva do sistema do país terceiro no seu conjunto, incluindo o conteúdo da proteção da privacidade e a sua aplicação e execução efetivas.

Além disso, o Tribunal esclareceu que a avaliação da Comissão não se deve limitar ao quadro geral de proteção de dados do país terceiro, devendo também incluir as regras que regem o acesso aos dados pessoais pelas autoridades públicas, em especial para efeitos de aplicação da lei e de segurança nacional[24]. Utilizando a Carta dos Direitos Fundamentais como referência, o Tribunal identificou vários requisitos que estas regras devem respeitar para cumprir a norma de «equivalência essencial». Por exemplo, a legislação neste domínio deve estabelecer regras claras e precisas que regulem o âmbito e a aplicação de uma medida e imponham exigências mínimas, de modo que as pessoas cujos dados pessoais estejam em causa disponham de garantias suficientes que permitam proteger eficazmente os seus dados contra os riscos de abuso e contra qualquer acesso e utilização ilícita dos mesmos[25]. Deverá também proporcionar às pessoas a possibilidade de recorrerem a vias de recurso para terem acesso aos dados pessoais que lhes digam respeito, ou para obterem a retificação ou a supressão de tais dados[26].

O RGPD baseou-se nos esclarecimentos prestados pelo Tribunal de Justiça, estabelecendo um catálogo pormenorizado de elementos que a Comissão tem de ter em conta numa avaliação da adequação[27]. Além disso, no seu acórdão de 16 de julho de 2020 no processo Schrems II, o Tribunal de Justiça aprofundou a norma de «equivalência essencial», em especial no que diz respeito às regras relativas ao acesso a dados pessoais por parte das autoridades públicas para efeitos de aplicação da lei e de segurança nacional. Em especial, esclareceu que a norma de

[21] O Comité Europeu para a Proteção de Dados reúne as autoridades de controlo da proteção de dados dos Estados-Membros e a Autoridade Europeia para a Proteção de Dados.
[22] Schrems I), n.os 73, 74 e 96. Ver também o considerando 104 do Regulamento (UE) 2016/679, que remete para a norma de equivalência essencial.
[23] Schrems I, n.º 74.
[24] Schrems I, n.º 90.
[25] Schrems I, n.º 91.
[26] Schrems I, n.º 95.
[27] Artigo 45.º, n.º 2, do RGPD.

«equivalência essencial» exige que os quadros jurídicos pertinentes que vinculam as autoridades públicas dos países e territórios terceiros em causa incluam garantias mínimas que assegurem que essas autoridades não possam aceder aos dados para além do necessário e proporcionado a fim de prosseguir objetivos legítimos e que os titulares dos dados gozem de direitos efetivos e oponíveis a essas autoridades[28].

A evolução do padrão de adequação reflete-se igualmente nas orientações inicialmente adotadas pelo Grupo de Trabalho do artigo 29.º e posteriormente aprovadas pelo CEPD[29]. Estas orientações e, em especial, o denominado «documento de referência relativo à adequação» clarificam melhor os elementos que a Comissão tem de ter em conta ao efetuar uma avaliação da adequação, nomeadamente fornecendo uma visão geral das «garantias essenciais» de acesso aos dados pessoais por parte das autoridades públicas. Estas últimas baseiam-se, em especial, na jurisprudência do Tribunal Europeu dos Direitos Humanos e foram atualizadas pelo CEPD para ter em conta os esclarecimentos prestados pelo Tribunal de Justiça no acórdão Schrems II[30]. Importa salientar que o documento de referência relativo à adequação também reconhece que a norma de «equivalência essencial» não implica uma reprodução ponto a ponto («fotocópia») das regras da UE, uma vez que os meios para assegurar um nível de proteção comparável podem variar entre os diferentes sistemas de privacidade, refletindo frequentemente tradições jurídicas diferentes.

Por conseguinte, para determinar se as 11 decisões de adequação adotadas ao abrigo das regras anteriores continuam a cumprir a norma estabelecida pelo RGPD, a Comissão teve em conta não só a evolução dos quadros de proteção de dados nos países e territórios em causa, mas também a evolução da interpretação, ao abrigo do direito da UE, do próprio padrão de adequação. Tal inclui igualmente uma avaliação do quadro jurídico que rege o acesso e a utilização de dados pessoais transferidos da UE pelas autoridades públicas dos países ou territórios que se considerou proporcionarem um nível de proteção adequado com base no artigo 25.º, n.º 6, da Diretiva Proteção de Dados.

3. PROCESSO DE REVISÃO

Conforme descrito acima, para cada um dos países ou territórios em causa, a avaliação das decisões de adequação em vigor abrange o quadro de proteção de dados e qualquer evolução relativamente a esse quadro jurídico desde a adoção da conclusão de adequação, bem como as regras que regem o acesso do governo aos dados — em especial, para efeitos de aplicação da lei e de segurança nacional. Nos últimos anos, os serviços da Comissão tomaram várias medidas para realizar a avaliação em causa, em estreita cooperação com cada um dos países ou territórios pertinentes.

[28] Schrems II, n.os 180 a 182.
[29] Documento de referência relativo à adequação, WP 254 rev.01, 6 de fevereiro de 2018 (disponível em: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108).
[30] Recomendações 02/2020 sobre as garantias essenciais europeias relativas às medidas de vigilância (disponíveis em: https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-022020-european-essential-guarantees_pt).

Para assistir a Comissão no cumprimento das obrigações de controlo que lhe assistem, cada um dos 11 países ou territórios forneceu informações exaustivas sobre a evolução do seu regime de proteção de dados desde a adoção da decisão de adequação. Além disso, a Comissão procurou obter, junto de cada um dos 11 países ou territórios, informações pormenorizadas sobre as regras em matéria de acesso governamental aos dados pessoais, em especial para efeitos de aplicação da lei e de segurança nacional, aplicáveis no país ou território pertinente. A Comissão procurou igualmente obter informações junto de fontes públicas, autoridades de supervisão e autoridades responsáveis pela aplicação da lei, bem como de peritos locais, sobre a aplicação das decisões e as alterações importantes da legislação e das práticas de cada um dos países e territórios em causa, tanto no que diz respeito às regras em matéria de proteção de dados aplicáveis aos operadores privados como no que se refere ao acesso governamental. Por último, sempre que pertinente, foram devidamente tidos em conta os compromissos internacionais subscritos por esses países/territórios ao abrigo de instrumentos regionais ou universais.

Nesta base, a Comissão encetou um diálogo intenso com cada um dos países e territórios em causa. No contexto deste diálogo, muitos desses países e territórios modernizaram e reforçaram a sua legislação em matéria de privacidade através de reformas abrangentes ou parciais (por exemplo, Andorra, Canadá, Ilhas Faroé, Suíça e Nova Zelândia) motivadas, nomeadamente, pela necessidade de assegurar a continuidade das decisões de adequação. Alguns destes países adotaram regulamentos e/ou orientações emanados da respetiva autoridade de proteção de dados para introduzir novos requisitos em matéria de proteção de dados (por exemplo, Israel e Uruguai) ou para clarificar determinadas regras em matéria de privacidade (por exemplo, Argentina, Canadá, Guernesey, Jersey, Ilha de Man, Israel e Nova Zelândia), com base nas práticas de execução ou na jurisprudência. Além disso, a fim de colmatar as diferenças pertinentes no que se refere ao nível de proteção, foram negociadas e acordadas garantias adicionais para os dados pessoais transferidos da Europa, sempre que necessário para assegurar a continuidade da decisão de adequação, com alguns dos países e territórios em causa. Por exemplo, o Governo canadiano alargou os direitos de acesso e de correção no que diz respeito aos dados pessoais tratados pelo setor público a todas as pessoas singulares, independentemente da sua nacionalidade ou local de residência (enquanto, no passado, estes direitos só estavam disponíveis para cidadãos canadianos, residentes permanentes ou pessoas presentes no Canadá)[31]. A título de exemplo adicional, o Governo israelita introduziu garantias específicas para reforçar a proteção dos dados pessoais transferidos do Espaço Económico Europeu que, nomeadamente, criam novas obrigações no domínio da exatidão e conservação dos dados, reforçam os direitos à informação e ao apagamento e introduzem categorias adicionais de dados sensíveis[32].

Paralelamente, os serviços da Comissão recolheram os pontos de vista e informaram regularmente o Parlamento Europeu (Comissão das Liberdades Cívicas, da Justiça e dos

[31] N.º 12 da Lei relativa à proteção da vida privada, Decreto de extensão n.º 1 e Decreto de extensão n.º 2.
[32] Regulamentos relativos à proteção da vida privada (Instruções relativas aos dados transferidos para Israel do Espaço Económico Europeu), 5783-2023, publicados no Jornal Oficial de Israel (*Reshumut*) em 7 de maio de 2023.

Assuntos Internos)[33], o Conselho (através do Grupo de Trabalho para a Proteção de Dados)[34], o CEPD[35] e o Grupo de Peritos Multilateral do RGPD[36] (que inclui representantes da sociedade civil, da indústria e do meio académico e profissionais da justiça) sobre os progressos da avaliação.

O presente relatório e o documento de trabalho dos serviços da Comissão (SWD) que o acompanha são, por conseguinte, o resultado de uma estreita cooperação com cada um dos países e territórios em causa, bem como da consulta e das reações das instituições e organismos competentes da UE. Baseiam-se em diversas fontes, incluindo legislação, atos regulamentares, jurisprudência, decisões e orientações das autoridades de proteção de dados, relatórios de organismos de supervisão (independentes) e contributos de partes interessadas. Antes da adoção do presente relatório, todos os países e territórios supracitados tiveram a oportunidade de verificar a exatidão factual das informações fornecidas sobre o seu sistema no documento de trabalho dos serviços da Comissão.

4. PRINCIPAIS CONSTATAÇÕES E CONCLUSÕES

A primeira revisão demonstrou, desde a adoção das decisões de adequação, uma maior convergência dos quadros de proteção de dados em vigor em cada um dos 11 países ou territórios com o quadro da UE. Além disso, no domínio do acesso governamental aos dados pessoais, a primeira revisão mostrou que a legislação destes países ou territórios impõe limitações e garantias adequadas e prevê mecanismos de supervisão e de recurso neste domínio.

As constatações pormenorizadas relativas a cada um dos 11 países ou territórios são apresentadas no documento de trabalho dos serviços da Comissão que acompanha o presente relatório. Com base nestas constatações, a Comissão conclui que cada um dos 11 países e territórios continua a assegurar um nível adequado de proteção dos dados pessoais transferidos da União Europeia na aceção do RGPD, conforme interpretado pelo Tribunal de Justiça. As constatações relativas a cada um dos países e territórios adequados são resumidas a seguir.

4.1. Andorra

A Comissão congratula-se com a evolução do quadro jurídico de Andorra desde a adoção da decisão de adequação, incluindo as alterações legislativas e as atividades dos organismos de supervisão. Em especial, a adoção da Lei Qualificada n.º 29/2021 relativa à proteção de dados pessoais, que entrou em vigor em maio de 2022, contribuiu para um nível mais elevado de

[33] Ver, por exemplo, a Resolução do Parlamento Europeu, de 25 de março de 2021, sobre o relatório de avaliação da Comissão sobre a execução do Regulamento Geral sobre a Proteção de Dados dois anos após a sua aplicação [2020/2717(RSP)], disponível na seguinte ligação: https://www.europarl.europa.eu/doceo/document/TA-9-2021-0111_PT.html.

[34] Ver, por exemplo, a Posição e constatações do Conselho sobre a aplicação do Regulamento Geral sobre a Proteção de Dados (RGPD), adotadas em 19 de dezembro de 2019, disponíveis na seguinte ligação: https://data.consilium.europa.eu/doc/document/ST-14994-2019-REV-1/pt/pdf.

[35] Ver, por exemplo, o documento intitulado *Contribution of the EDPB to the evaluation of the GDPR under Article 97* (não traduzido para português), adotado em 18 de fevereiro de 2020, disponível na seguinte ligação: https://edpb.europa.eu/sites/default/files/files/file1/edpb_contributiongdprevaluation_20200218.pdf.

[36] Ver, por exemplo, o relatório do Grupo de Peritos Multilateral sobre a avaliação do RGPD, disponível na seguinte ligação: https://ec.europa.eu/transparency/expert-groups-register/screen/meetings/consult?lang=pt&do=groupDetail.groupMeeting&meetingId=21356.

proteção de dados, uma vez que a lei está estreitamente alinhada com o RGPD na sua estrutura e nas suas principais componentes.

No domínio do acesso governamental aos dados pessoais, as autoridades públicas de Andorra estão sujeitas a regras claras, precisas e acessíveis ao abrigo das quais podem aceder aos dados transferidos da UE e, subsequentemente, utilizá-los para objetivos de interesse público, em especial para efeitos de aplicação do direito penal e de segurança nacional. Estas limitações e garantias decorrem do quadro jurídico global e dos compromissos internacionais, nomeadamente a Constituição de Andorra, a Convenção Europeia dos Direitos Humanos (CEDH) e a Convenção do Conselho da Europa para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal (Convenção 108 e Protocolo de alteração, que cria a Convenção 108+ modernizada), bem como das regras específicas de proteção de dados aplicáveis ao tratamento de dados pessoais no contexto da aplicação da lei, que reproduzem essencialmente os elementos fundamentais da Diretiva (UE) 2016/680[37]. Além disso, a legislação de Andorra impõe uma série de condições e limitações específicas ao acesso e à utilização de dados pessoais pelas autoridades públicas e prevê mecanismos de supervisão e de recurso neste domínio.

Com base nas constatações gerais apresentadas no documento de trabalho dos serviços da Comissão, a Comissão conclui que Andorra continua a proporcionar um nível adequado de proteção dos dados pessoais transferidos da UE.

No que diz respeito às regras específicas de proteção de dados atualmente aplicáveis ao tratamento de dados pelas autoridades responsáveis pela aplicação da lei, a Comissão congratula-se com a intenção do legislador de Andorra de substituir estas regras por um regime mais abrangente, que será ainda mais alinhado com as regras aplicáveis na UE. A Comissão acompanhará de perto a evolução futura neste domínio.

4.2. Argentina

A Comissão congratula-se com a evolução do quadro jurídico argentino desde a adoção da decisão de adequação, incluindo alterações legislativas, jurisprudência e atividades dos organismos de supervisão, que contribuíram para um nível mais elevado de proteção de dados. Em especial, a independência da autoridade de controlo da proteção de dados argentina foi significativamente reforçada pelo Decreto n.º 746/17, que confiou à *Agencia de Acceso a la Información Pública* (AAIP) a responsabilidade de supervisionar o cumprimento da legislação em matéria de proteção de dados. Além disso, a AAIP emitiu uma série de regulamentos e pareceres vinculativos que clarificam a forma como o quadro de proteção de dados deve ser interpretado e aplicado na prática, contribuindo assim para manter atualizada a legislação em matéria de proteção de dados. A Argentina reforçou igualmente os seus compromissos internacionais no domínio da proteção de dados ao aderir, em 2019, à Convenção do Conselho da Europa para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados

[37] Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho.

de Caráter Pessoal e ao seu Protocolo Adicional e ao ratificar, em 2023, o Protocolo de alteração que cria a Convenção 108+ modernizada.

No domínio do acesso governamental aos dados pessoais, as autoridades públicas da Argentina estão sujeitas a regras claras, precisas e acessíveis ao abrigo das quais podem aceder aos dados transferidos da UE e, subsequentemente, utilizá-los para objetivos de interesse público, em especial para efeitos de aplicação do direito penal e de segurança nacional. Estas limitações e garantias decorrem do quadro jurídico global e dos compromissos internacionais, nomeadamente a Constituição argentina, a Convenção Americana sobre Direitos Humanos, a Convenção 108 e a Convenção 108+, bem como das regras argentinas em matéria de proteção de dados (Lei n.º 25.326 relativa à proteção de dados pessoais, de 4 de outubro de 2000), que são igualmente aplicáveis ao tratamento de dados pessoais pelas autoridades públicas argentinas, nomeadamente para efeitos de aplicação da lei e de segurança nacional. Além disso, a legislação argentina impõe uma série de condições e limitações específicas ao acesso e à utilização de dados pessoais para efeitos de aplicação do direito penal e de segurança nacional e prevê mecanismos de supervisão e de recurso neste domínio.

Com base nas constatações gerais apresentadas no documento de trabalho dos serviços da Comissão, a Comissão conclui que a Argentina continua a proporcionar um nível adequado de proteção dos dados pessoais transferidos da UE.

Simultaneamente, a Comissão recomenda a consagração na legislação das proteções desenvolvidas a nível sublegislativo, a fim de reforçar a segurança jurídica e consolidar estes requisitos. O projeto de lei sobre a proteção de dados recentemente apresentado ao Congresso argentino poderá constituir uma oportunidade para codificar essa evolução e, assim, reforçar ainda mais o quadro de privacidade argentino. A Comissão acompanhará de perto a evolução futura neste domínio.

4.3. Canadá

A Comissão congratula-se com a evolução do quadro jurídico canadiano desde a adoção da decisão de adequação, incluindo várias alterações legislativas, jurisprudência e atividades dos organismos de supervisão, que contribuíram para um nível mais elevado de proteção de dados. Em especial, a Lei relativa à proteção de informações pessoais e documentos eletrónicos (PIPEDA) foi reforçada através de diversas alterações (por exemplo, no que se refere às condições para o consentimento válido e às notificações de violação de dados), tendo os principais requisitos em matéria de proteção de dados (por exemplo, sobre o tratamento de dados sensíveis) sido clarificados através da jurisprudência, bem como de orientações emitidas pela autoridade federal canadiana de proteção de dados, o *Office of the Privacy Commissioner* (Gabinete do Comissário para a Proteção da Vida Privada). Simultaneamente, a Comissão recomenda a consagração na legislação de algumas das proteções desenvolvidas a nível sublegislativo, a fim de reforçar a segurança jurídica e consolidar estes requisitos. A reforma legislativa em curso da PIPEDA poderá, nomeadamente, constituir uma oportunidade para codificar essa evolução e, assim, reforçar ainda mais o quadro de privacidade canadiano. A Comissão acompanhará de perto a evolução futura neste domínio.

No domínio do acesso governamental aos dados pessoais, as autoridades públicas do Canadá estão sujeitas a regras claras, precisas e acessíveis ao abrigo das quais podem aceder aos dados transferidos da UE e, subsequentemente, utilizá-los para objetivos de interesse público, em especial para efeitos de aplicação do direito penal e de segurança nacional. Estas limitações e garantias decorrem do quadro constitucional global (a Carta dos Direitos e das Liberdades do Canadá), da jurisprudência e da legislação específica que regula o acesso aos dados, bem como das regras em matéria de proteção de dados (ou seja, a Lei relativa à proteção de informações pessoais e leis semelhantes a nível provincial) que também se aplicam ao tratamento de dados pessoais pelas autoridades públicas canadianas, nomeadamente para efeitos de aplicação da lei e de segurança nacional. Além disso, o sistema jurídico canadiano prevê mecanismos eficazes de supervisão e de recurso neste domínio, nomeadamente através de um recente alargamento dos direitos dos titulares dos dados e das possibilidades de recurso aos nacionais ou residentes não canadianos.

Com base nas constatações gerais apresentadas no documento de trabalho dos serviços da Comissão, a Comissão conclui que o Canadá continua a proporcionar um nível adequado de proteção dos dados pessoais transferidos da UE para destinatários sujeitos à PIPEDA. Como referido acima, a PIPEDA está atualmente a ser objeto de uma reforma legislativa que poderá reforçar ainda mais a proteção da privacidade, nomeadamente em domínios pertinentes para a conclusão de adequação.

4.4. Ilhas Faroé

A Comissão congratula-se com a evolução do quadro jurídico das Ilhas Faroé desde a adoção da decisão de adequação, incluindo alterações legislativas, jurisprudência e atividades dos organismos de supervisão, que contribuíram para um nível mais elevado de proteção de dados. Em especial, as Ilhas Faroé modernizaram significativamente o seu quadro de proteção de dados através da adoção da Lei de Proteção de Dados, que entrou em vigor em 2021 e alinhou estreitamente o regime das Ilhas Faroé com o RGPD.

No domínio do acesso governamental aos dados pessoais, as autoridades públicas das Ilhas Faroé estão sujeitas a regras claras, precisas e acessíveis ao abrigo das quais podem aceder aos dados transferidos da UE e, subsequentemente, utilizá-los para objetivos de interesse público, em especial para efeitos de aplicação do direito penal e de segurança nacional. Estas limitações e garantias decorrem do quadro jurídico global e dos compromissos internacionais, nomeadamente o quadro constitucional e a CEDH, bem como de leis específicas que regulam o acesso governamental aos dados e das regras de proteção de dados aplicáveis ao tratamento de dados pessoais para efeitos de aplicação do direito penal [Lei relativa ao tratamento de dados pessoais pelas autoridades responsáveis pela aplicação da lei, que entrou em vigor nas Ilhas Faroé em 2022 e transpõe a legislação adotada pela Dinamarca para aplicar a Diretiva (UE) 2016/680 nas Ilhas Faroé] e de segurança nacional (contidas na Lei relativa ao Serviço de Informações de Segurança). Além disso, estão disponíveis mecanismos eficazes de supervisão e de recurso neste domínio.

Com base nas constatações gerais apresentadas no documento de trabalho dos serviços da Comissão, a Comissão conclui que as Ilhas Faroé continuam a proporcionar um nível adequado de proteção dos dados pessoais transferidos da UE.

4.5. Guernesey

A Comissão congratula-se com a evolução do quadro jurídico de Guernesey desde a adoção da decisão de adequação, incluindo alterações legislativas e atividades dos organismos de supervisão, que contribuíram para um nível mais elevado de proteção de dados. Em especial, Guernesey modernizou significativamente o seu quadro de proteção de dados através da adoção da Lei de Proteção de Dados (Bailiado de Guernesey) de 2017, que é aplicável desde 2019, e que alinha estreitamente o regime de Guernesey com o RGPD.

No domínio do acesso governamental aos dados pessoais, as autoridades públicas de Guernesey estão sujeitas a regras claras, precisas e acessíveis ao abrigo das quais podem aceder aos dados transferidos da UE e, subsequentemente, utilizá-los para objetivos de interesse público, em especial para efeitos de aplicação do direito penal e de segurança nacional. Estas limitações e garantias decorrem do quadro jurídico global e dos compromissos internacionais, nomeadamente a CEDH e a Convenção 108, bem como das regras de proteção de dados de Guernesey, incluindo as disposições específicas para o tratamento de dados pessoais no contexto da aplicação da lei estabelecidas na Portaria de 2018 sobre a proteção de dados (aplicação da lei e questões conexas) (Bailiado de Guernesey). Além disso, a legislação de Guernesey impõe uma série de condições e limitações específicas ao acesso e à utilização de dados pessoais para efeitos de aplicação do direito penal e de segurança nacional e prevê mecanismos de supervisão e de recurso neste domínio.

Com base nas constatações gerais apresentadas no documento de trabalho dos serviços da Comissão, a Comissão conclui que Guernesey continua a proporcionar um nível adequado de proteção dos dados pessoais transferidos da UE.

4.6. Ilha de Man

A Comissão congratula-se com a evolução do quadro jurídico manês desde a adoção da decisão de adequação, incluindo alterações legislativas e atividades dos organismos de supervisão, que contribuíram para um nível mais elevado de proteção de dados. Em especial, a Ilha de Man adotou nova legislação em 2018 [a Lei de Proteção de Dados de 2018, complementada pelo Decreto de 2018 sobre a proteção de dados (aplicação do RGPD)], que incorpora a maioria das disposições do quadro de proteção de dados da UE na ordem jurídica manesa, introduzindo simultaneamente apenas pequenos ajustamentos em aspetos específicos, em especial para adaptar o quadro ao contexto local.

No domínio do acesso governamental aos dados pessoais, as autoridades públicas da Ilha de Man estão sujeitas a regras claras, precisas e acessíveis ao abrigo das quais podem aceder aos dados transferidos da UE e, subsequentemente, utilizá-los para objetivos de interesse público, em especial para efeitos de aplicação do direito penal e de segurança nacional. Estas limitações e garantias decorrem do quadro jurídico global e dos compromissos internacionais,

nomeadamente a CEDH e a Convenção 108, bem como das regras de proteção de dados manesas, incluindo as disposições específicas para o tratamento de dados pessoais no contexto da aplicação da lei estabelecidas no Decreto de 2018 sobre a proteção de dados (aplicação da Diretiva Proteção de Dados na Aplicação da Lei) e nos regulamentos de execução de 2018 da Diretiva Proteção de Dados na Aplicação da Lei. Além disso, a legislação manesa impõe uma série de limitações específicas ao acesso e à utilização de dados pessoais para efeitos de aplicação do direito penal e de segurança nacional e prevê mecanismos de supervisão e de recurso neste domínio.

Com base nas constatações gerais apresentadas no documento de trabalho dos serviços da Comissão, a Comissão conclui que a Ilha de Man continua a proporcionar um nível adequado de proteção dos dados pessoais transferidos da UE.

4.7. Israel

A Comissão congratula-se com a evolução do quadro jurídico israelita desde a adoção da decisão de adequação, incluindo alterações legislativas, jurisprudência e atividades dos organismos de supervisão, que contribuíram para um nível mais elevado de proteção de dados. Em especial, Israel introduziu garantias específicas a fim de reforçar a proteção dos dados pessoais transferidos do Espaço Económico Europeu através da adoção de regulamentos relativos à proteção da privacidade (instruções para os dados transferidos para Israel do Espaço Económico Europeu), 5783-2023. Israel reforçou igualmente os requisitos em matéria de segurança dos dados através da adoção de regulamentos relativos à proteção da privacidade (segurança dos dados), 5777-2017, tendo consolidado a independência da sua autoridade de controlo da proteção de dados numa resolução governamental vinculativa.

No domínio do acesso governamental aos dados pessoais, as autoridades públicas de Israel estão sujeitas a regras claras, precisas e acessíveis ao abrigo das quais podem aceder aos dados transferidos da UE e, subsequentemente, utilizá-los para objetivos de interesse público, em especial para efeitos de aplicação do direito penal e de segurança nacional. Estas limitações e garantias decorrem do quadro jurídico global, nomeadamente da Lei Fundamental israelita, bem como da Lei de Proteção da Privacidade, 5741-1981, e dos regulamentos adotados no seu âmbito, que se aplicam ao tratamento de dados pessoais pelas autoridades públicas israelitas, nomeadamente para efeitos de aplicação da lei e de segurança nacional. Além disso, a legislação israelita impõe uma série de limitações específicas ao acesso e à utilização de dados pessoais para efeitos de aplicação do direito penal e de segurança nacional e prevê mecanismos de supervisão e de recurso neste domínio.

Com base nas constatações gerais apresentadas no documento de trabalho dos serviços da Comissão, a Comissão conclui que Israel continua a proporcionar um nível adequado de proteção dos dados pessoais transferidos da UE.

Simultaneamente, a Comissão recomenda a consagração na legislação das proteções desenvolvidas a nível sublegislativo e pela jurisprudência, a fim de reforçar a segurança jurídica e consolidar estes requisitos. O projeto de lei sobre a proteção da privacidade (alteração n.º 14), 5722-2022, recentemente apresentado ao Parlamento israelita, constitui uma importante

oportunidade para consolidar e codificar essa evolução e, assim, reforçar ainda mais o quadro de privacidade israelita. A Comissão acompanhará de perto a evolução futura neste domínio.

4.8. Jersey

A Comissão congratula-se com a evolução do quadro jurídico de Jersey desde a adoção da decisão de adequação, incluindo alterações legislativas, jurisprudência e atividades dos organismos de supervisão, que contribuíram para um nível mais elevado de proteção de dados. Em especial, Jersey modernizou significativamente o seu quadro de proteção de dados através da adoção da Lei de Proteção de Dados (Jersey) de 2018 e da Lei de 2018 que cria a autoridade de proteção de dados (Jersey), que entraram em vigor em 2018 e alinham estreitamente o regime de Jersey com o RGPD.

No domínio do acesso governamental aos dados pessoais, as autoridades públicas de Jersey estão sujeitas a regras claras, precisas e acessíveis ao abrigo das quais podem aceder aos dados transferidos da UE e, subsequentemente, utilizá-los para objetivos de interesse público, em especial para efeitos de aplicação do direito penal e de segurança nacional. Estas limitações e garantias decorrem do quadro jurídico global e dos compromissos internacionais, nomeadamente a CEDH e a Convenção 108, bem como das regras de proteção de dados de Jersey, incluindo as disposições específicas para o tratamento de dados pessoais no contexto da aplicação da lei estabelecidas na Lei de Proteção de Dados (Jersey) de 2018, com a redação que lhe foi dada pelo anexo 1 da referida lei. Além disso, a legislação de Jersey impõe uma série de limitações específicas ao acesso e à utilização de dados pessoais para efeitos de aplicação do direito penal e de segurança nacional e prevê mecanismos de supervisão e de recurso neste domínio.

Com base nas constatações gerais apresentadas no documento de trabalho dos serviços da Comissão, a Comissão conclui que Jersey continua a proporcionar um nível adequado de proteção dos dados pessoais transferidos da UE.

4.9. Nova Zelândia

A Comissão congratula-se com a evolução do quadro jurídico da Nova Zelândia desde a adoção da decisão de adequação, incluindo alterações legislativas, jurisprudência e atividades dos organismos de supervisão, que contribuíram para um nível mais elevado de proteção de dados. Em especial, o regime de proteção de dados foi objeto de uma reforma abrangente com a adoção da Lei de 2020 relativa à privacidade, que reforçou ainda mais a convergência com o quadro de proteção de dados da UE, nomeadamente no que diz respeito às regras aplicáveis às transferências internacionais de dados pessoais e aos poderes da autoridade de proteção de dados (*Office of the Privacy Commissioner*).

No domínio do acesso governamental aos dados pessoais, as autoridades públicas da Nova Zelândia estão sujeitas a regras claras, precisas e acessíveis ao abrigo das quais podem aceder aos dados transferidos da UE e, subsequentemente, utilizá-los para objetivos de interesse público, em especial para efeitos de aplicação do direito penal e de segurança nacional. Estas limitações e garantias decorrem do quadro constitucional global (por exemplo, a Lei da Carta

dos Direitos dos Cidadãos) e da jurisprudência, bem como de leis específicas que regulam o acesso governamental aos dados e de disposições da Lei relativa à privacidade que também se aplicam ao tratamento de dados pessoais pelas autoridades responsáveis pela aplicação do direito penal e pela segurança nacional. Além disso, o sistema jurídico neozelandês prevê diferentes mecanismos de supervisão e de recurso neste domínio.

Com base nas constatações gerais apresentadas no documento de trabalho dos serviços da Comissão, a Comissão conclui que a Nova Zelândia continua a proporcionar um nível adequado de proteção dos dados pessoais transferidos da UE. A Comissão congratula-se igualmente com a recente apresentação de um projeto de lei ao Parlamento pelo Governo neozelandês para alterar a Lei de 2020 relativa à privacidade, a fim de reforçar ainda mais os requisitos de transparência existentes. A Comissão acompanhará de perto a evolução futura neste domínio.

4.10. Suíça

A Comissão congratula-se com a evolução do quadro jurídico suíço desde a adoção da decisão de adequação, incluindo alterações legislativas, jurisprudência e atividades dos organismos de supervisão, que contribuíram para um nível mais elevado de proteção de dados. Em especial, a Lei Federal de Proteção de Dados modernizada reforçou ainda mais a convergência com o quadro de proteção de dados da UE, nomeadamente no que diz respeito à proteção de dados sensíveis e às regras relativas às transferências internacionais de dados. A Suíça reforçou igualmente os seus compromissos internacionais no domínio da proteção de dados através da ratificação, em setembro de 2023, da Convenção 108+.

No domínio do acesso governamental aos dados pessoais, as autoridades públicas da Suíça estão sujeitas a regras claras, precisas e acessíveis ao abrigo das quais podem aceder aos dados transferidos da UE e, subsequentemente, utilizá-los para objetivos de interesse público, em especial para efeitos de aplicação do direito penal e de segurança nacional. Estas limitações e garantias decorrem do quadro jurídico global e dos compromissos internacionais, nomeadamente a Constituição Federal Suíça, a CEDH e a Convenção 108+, bem como das regras suíças em matéria de proteção de dados, incluindo a Lei Federal de Proteção de Dados e as regras específicas de proteção de dados aplicáveis às autoridades responsáveis pela aplicação do direito penal (por exemplo, o Código de Processo Penal) e às autoridades nacionais de segurança (por exemplo, a Lei relativa ao Serviço de Informações). Além disso, a legislação suíça impõe uma série de limitações específicas ao acesso e à utilização de dados pessoais para efeitos de aplicação do direito penal e de segurança nacional e prevê mecanismos de supervisão e de recurso neste domínio.

Com base nas constatações gerais apresentadas no documento de trabalho dos serviços da Comissão, a Comissão conclui que a Suíça continua a proporcionar um nível adequado de proteção dos dados pessoais transferidos da UE.

4.11. Uruguai

A Comissão congratula-se com a evolução do quadro jurídico do Uruguai desde a adoção da decisão de adequação, incluindo várias alterações legislativas, jurisprudência e atividades dos

organismos de supervisão, que contribuíram para um nível mais elevado de proteção de dados. Em especial, o Uruguai modernizou e reforçou a sua Lei n.º 18.331 de proteção de dados pessoais e ação de *habeas data*, de 2008, através da adoção de alterações legislativas em 2018 e 2020 que alargaram o âmbito territorial da legislação em matéria de proteção de dados, criaram novos requisitos de responsabilização (como avaliações de impacto, proteção de dados desde a conceção e por defeito, notificação de violações de dados e nomeação de encarregados da proteção de dados) e introduziram proteções adicionais para os dados biométricos. O Uruguai reforçou igualmente os seus compromissos internacionais no domínio da proteção de dados ao aderir à Convenção 108 em 2019 e ao ratificar a Convenção 108+ em 2021.

No domínio do acesso governamental aos dados pessoais, as autoridades públicas do Uruguai estão sujeitas a regras claras, precisas e acessíveis ao abrigo das quais podem aceder aos dados transferidos da UE e, subsequentemente, utilizá-los para objetivos de interesse público, em especial para efeitos de aplicação do direito penal e de segurança nacional. Estas limitações e garantias decorrem do quadro jurídico global e dos compromissos internacionais, nomeadamente a Constituição uruguaia, a Convenção Americana sobre Direitos Humanos, a Convenção 108 e a Convenção 108+, bem como das regras em matéria de proteção de dados constantes da Lei n.º 18.331 de proteção de dados pessoais e ação de *habeas data*, que se aplicam ao tratamento de dados pessoais pelas autoridades públicas do Uruguai, nomeadamente para efeitos de aplicação da lei e de segurança nacional. Além disso, a legislação do Uruguai impõe uma série de condições e limitações específicas ao acesso e à utilização de dados pessoais pelas autoridades públicas e prevê mecanismos de supervisão e de recurso neste domínio.

Com base nas constatações gerais formuladas no âmbito desta primeira revisão, a Comissão conclui que o Uruguai continua a proporcionar um nível adequado de proteção dos dados pessoais transferidos da UE.

5. ACOMPANHAMENTO E COOPERAÇÃO FUTUROS

A Comissão reconhece e valoriza muito a excelente cooperação com as autoridades competentes de cada um dos países e territórios em causa na realização da revisão em questão. A Comissão continuará a acompanhar de perto a evolução dos quadros de proteção e das práticas efetivas dos países e territórios em causa. Caso se registe uma evolução num país ou território referido que afete negativamente o nível de proteção de dados considerado adequado, a Comissão recorrerá, se necessário, aos poderes que lhe são conferidos pelo artigo 45.º, n.º 5, do RGPD para suspender, alterar ou retirar uma decisão de adequação.

A revisão em causa confirma que a adoção de uma decisão de adequação não é um «ponto final», mas proporciona uma oportunidade para intensificar ainda mais o diálogo e a cooperação com parceiros internacionais que partilham a mesma visão sobre fluxos de dados e questões digitais em geral. Neste contexto, a Comissão aguarda com expectativa futuros intercâmbios com as autoridades competentes para reforçar ainda mais a cooperação a nível internacional na promoção da circulação livre e segura de fluxos de dados, nomeadamente através do reforço da cooperação em matéria de aplicação da lei. Para intensificar este diálogo e promover o intercâmbio de informações e a experiência, a Comissão tenciona organizar, em 2024, uma

reunião de alto nível que reunirá representantes da UE e de todos os países que beneficiam de uma decisão de adequação.