O RGPD E A SUA APLICAÇÃO TRANSFRONTEIRIÇA: ATÉ ONDE ESTÃO PROTEGIDOS OS NOSSOS DADOS PESSOAIS?[1]

Sónia Moreira[2]
https://doi.org/10.21814/uminho.ed.151.20

Resumo: É possível que já tenhamos passado pela experiência de termos tido de ceder os nossos dados pessoais para podermos aceder a um serviço ou a um bem transacionado por um fornecedor de fora da União Europeia (UE). O risco inerente a este tipo de contratação é elevado, uma vez que o RGPD poderá não ser aplicável na situação referida. O objetivo deste texto é analisar a protecção conferida pelo RGPD fora da UE, nomeadamente, à luz do novo Quadro de Privacidade dos Dados UE-EUA, adoptado em 10 de julho de 2023, no que toca às relações privadas.

Palavras-chave: RGPD; aplicação transfronteiriça; Quadro de Privacidade dos Dados UE-EUA.

[1] O presente texto foi entregue para publicação no número temático sobre Protecção de Dados Pessoais da *Revista do CEJ* (nº II-2023).

[2] Docente da Escola da Direito da Universidade do Minho e Investigadora Integrada do JusGov.

1. O RGPD: breves notas gerais quanto à sua adopção

Originalmente, o regime jurídico da protecção de dados no seio da UE constava da Directiva 95/46/CE, de 24 de Outubro, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados[3], transposta para o ordenamento português através da Lei nº 67/98, de 26 de Outubro[4]. No entanto, a sociedade alterou-se radicalmente com o desenvolvimento tecnológico sem precedentes a que assistimos nas últimas décadas, tendo a contratação eletrónica superado todas as expectativas. Este facto sofreu ainda um agravamento exponencial mais recentemente, em grande medida por os consumidores se terem habituado a contratar *online*, como consequência da restrição às deslocações, imposta por razões sanitárias no contexto da pandemia. Ora, para poderem adquirir bens *online* ou contratar a prestação de serviços, é sempre necessário, ao menos, permitir certas operações de tratamento de dados pessoais, no mínimo, relativos à facturação.

Nos termos do art. 2º, al. a), da Directiva, entendia-se como dado pessoal "qualquer informação relativa a uma pessoa singular identificada ou identificável", considerando-se "identificável todo aquele que [pudesse] ser identificado, directa ou indirectamente, nomeadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social". A doutrina costumava elencar a respeito da interpretação desta norma, dados como o

[3] Parlamento Europeu/Conselho da União Europeia, «Directiva 95/46/CE do Parlamento Europeu e do Conselho de 24 de Outubro de 1995 relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados», *Jornal Oficial das Comunidades Europeias* [em linha], nº L 281 (23/11/1995), p. 0031-0050 [Consult. 13/7/2023]. Disponível na Internet: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A31995L0046.

[4] Designada como Lei da Protecção de Dados Pessoais. Nos termos desta lei portuguesa, só podia recolher-se e proceder-se ao tratamento dos dados pessoais não públicos de uma pessoa singular com vista a atingir determinadas finalidades, explícitas e legítimas, não podendo um tratamento posterior vir contrariar tais finalidades; a recolha só seria legítima se os dados em causa fossem adequados e pertinentes para as finalidades em causa e os dados só podiam ser conservados durante o período necessário à sua prossecução, a menos que estivessem em causa fins históricos, estatísticos ou científicos, mediante autorização da Comissão Nacional de Protecção de Dados, a requerimento do respectivo responsável pelo seu tratamento. Mais importante ainda, em regra, o tratamento só poderia realizar-se se o titular dos dados nele consentisse de forma inequívoca ou caso se verificasse uma das excepções previstas na lei. Sobre este regime em geral, com especial enfoque no consentimento, v. Eva Sónia Moreira da Silva, «Como escapar às malhas da política de privacidade das redes sociais? Uma análise à luz da lei portuguesa», in Federico Bueno de Mata, *Fodertics II: Hacia una Justicia 2.0. Estudios sobre Derecho y Nuevas Tecnologías*, Salamanca, Ratio Legis Editiones, 2014, pp. 415 ss.

nome, a morada, o número de identificação civil, do passaporte, de identificação fiscal, o número de telefone ou telemóvel, o *e-mail*, o endereço de IP (*internet protocol*) do computador com que se acede à internet, a matrícula de um veículo, o valor da retribuição salarial, o som da voz registada, a história clínica, as classificações escolares, o *curriculum vitae*, o número de cartão de crédito, as compras efectuadas, imagens recolhidas por câmaras de vigilância, fotografias divulgadas na internet[5], etc. Ou seja, tudo aquilo que permitisse identificar uma pessoa era considerado um dado pessoal[6]. É fácil de ver que os dados que cedemos em sede de contratação electrónica cabiam aqui.

Mesmo antes da pandemia, no entanto, já se sentia que o regime jurídico da Diretiva não era suficiente para acautelar adequadamente os fluxos de dados dos cidadãos europeus, em particular quando negociavam com entidades de fora da UE. Por outro lado, o anterior regime, sendo baseado numa Directiva, permitia adaptações por parte dos diferentes Estados-Membros, dando azo à possibilidade de existirem diferenças nos níveis de proteçcão[7] dos dados pessoais de Estado-Membro para Estado-Membro[8].

Para resolver estas vulnerabilidades, vimos nascer em 2016, um novo regime, desta vez sob a forma de um Regulamento: o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016,

---

[5] Por exemplo, para além da própria imagem da pessoa, que é um dado biométrico, caso as fotografias em causa tenham associados os dados de localização geográfica, é possível vigiar o comportamento das pessoas (onde estão, com quem, com que frequência, etc.). Neste sentido, Catarina Sarmento e Castro, «A jurisprudência do Tribunal de Justiça da União Europeia, o Regulamento Geral sobre a proteção de dados pessoais e as novas perspectivas para o direito ao esquecimento na Europa», in Maria Lúcia Amaral (coord.), *Estudos em Homenagem ao Conselheiro Presidente Rui Moura Ramos*, vol. I, Coimbra, Almedina, 2016, p. 1056.

[6] Catarina Sarmento e Castro, *Direito da Informática, Privacidade e Dados Pessoais*, Coimbra, Almedina, 2005, pp. 74 e ss.

[7] A este respeito, v. Tiago Branco da Costa, «Proteção de dados pessoais: da Diretiva ao Regulamento Geral sobre a Proteção de Dados», in Isabel Celeste M. Fonseca [et al.], *Desafios do Direito no Século XXI: uma Reflexão Luso-Brasileira sob o Signo Interdisciplinar*, [S. l.], Escola de Direito da Universidade do Minho/JusGov, 2019, pp. 102-103.

[8] Neste sentido, o Considerando (9) do RGPD afirma que "[o]s objetivos e os princípios da Diretiva 95/46/CE (...) não evitaram a fragmentação da aplicação da proteção dos dados ao nível da União, nem a insegurança jurídica ou o sentimento generalizado da opinião pública de que subsistem riscos significativos para a proteção das pessoas singulares, nomeadamente no que diz respeito às atividades por via eletrónica. As diferenças no nível de proteção dos direitos e das pessoas singulares, nomeadamente do direito à proteção dos dados pessoais no contexto do tratamento desses dados nos Estados-Membros, podem impedir a livre circulação de dados pessoais na União. Essas diferenças podem, por conseguinte, constituir um obstáculo ao exercício das atividades económicas a nível da União, distorcer a concorrência e impedir as autoridades de cumprirem as obrigações que lhes incumbem por força do direito da União. Essas diferenças entre os níveis de proteção devem-se à existência de disparidades na execução e aplicação da Diretiva 95/46/CE".

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)[9]. Nos termos do seu art. 4º, al. 1), dados pessoais são "informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular". Assim, como vemos, a definição deste conceito à luz da nova regulamentação vai de encontro ao já defendido pela doutrina quanto à sua interpretação à luz do normativo fixado na anterior Directiva[10].

O Considerando (2) do RGPD, determina que "[o]s princípios e as regras em matéria de proteção das pessoas singulares relativamente ao tratamento dos seus dados pessoais deverão respeitar, independentemente da nacionalidade ou do local de residência dessas pessoas, os seus direitos e liberdades fundamentais, nomeadamente o direito à proteção dos dados pessoais". Por outro lado, o fluxo de dados é importante: pense-se na cooperação entre Estados (cfr. o Considerando (5), "[a]s autoridades nacionais dos Estados-Membros são chamadas, por força do direito da União, a colaborar e a trocar dados pessoais entre si, a fim de poderem desempenhar as suas funções ou executar funções por conta de uma autoridade de outro Estado-Membro"); pense-se na necessidade de acautelar a partilha de dados de saúde de um cidadão europeu que dá entrada num hospital de um Estado-Membro diferente do seu Estado-Membro de origem, por exemplo[11].

---

[9] Parlamento Europeu/Conselho da União Europeia – *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)* [em linha]. [Consult. 13/7/2023]. Disponível na Internet: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679.

[10] Neste sentido, Sónia Moreira, «A Protecção das Pessoas Singulares no Novo Regulamento Geral de Protecção de Dados Pessoais», in Clara Calheiros [et al.], *Direito na Lusofonia. Direito e Novas Tecnologias*, [S. l.], Escola de Direito da Universidade do Minho/JusGov, 2018, p. 489.

[11] A respeito dos dados de saúde, v. Tiago Branco da Costa, «O Altruísmo (Económico?) de Dados: Breves considerações sobre o Espaço Europeu de dados de Saúde e a Proteção de Dados Pessoais», in A. Sofia Pinto Oliveira/Patrícia Jerónimo, *Liber Amicorum Benedita Mac Crorie*, Braga, UMinho Editora, 2022, pp. 613 e ss.

Daí que o Considerando (3) do RGPD recorde que já a Directiva pretendia assegurar a "livre circulação de dados pessoais entre os Estados-Membros". Assim, apesar de se pretender proteger o direito à auto-determinação informacional de cada cidadão – o direito a decidir o que fazer dos seus dados pessoais, como um direito fundamental que decorre do direito mais geral à privacidade[12] – , a verdade é que também se reconhece que "[o] direito à proteção de dados pessoais não é absoluto; deve ser considerado em relação à sua função na sociedade e ser equilibrado com outros direitos fundamentais, em conformidade com o princípio da proporcionalidade", ou seja, é necessário encontrar um ponto de equilíbrio entre o direito à privacidade, o respeito pela vida pessoal e familiar, o respeito pelo domicílio e pelas comunicações, a proteção dos dados pessoais, a liberdade de pensamento, de consciência e de religião, a liberdade de expressão e de informação, etc. (Considerando (4)) e as necessidades de tratamento dos dados pessoais de maneira a que a livre circulação de pessoas, bens e serviços na UE possa funcionar devidamente. Adicionalmente, o facto de as próprias pessoas singulares disponibilizarem muitos dos seus dados voluntariamente em plataformas sociais e de as novas tecnologias facilitarem a sua divulgação e partilha torna mais difícil proteger os referidos direitos fundamentais.

Assim, o RGPD visou criar um quadro regulamentar sólido e mais coerente[13], a fim de "gerar a confiança necessária ao desenvolvimento da economia digital no conjunto do mercado interno". Para tanto, defende que "[a] s pessoas singulares deverão poder controlar a utilização que é feita dos seus dados pessoais" (Considerando (7)) e o nível de protecção concedido deve ser equivalente em todos os Estados-Membros (Considerando (10)). Daí a opção

[12] Entre nós, a este respeito, há quem defenda a existência de um direito à identidade informacional. V. Alexandre Sousa Pinheiro, *Privacy e Protecção de Dados Pessoais: a Construção dogmática do Direito à Identidade Informacional*, Lisboa, AAFDL, 2015, pp. 778 e ss. Defendendo, igualmente, que a protecção dos dados pessoais já consta do art. 35º da CRP, como direito fundamental, desde 1976, v. anotação ao art. 35º da CRP em José Joaquim Gomes Canotilho/ Vital Moreira, *Constituição da República Portuguesa Anotada*, vol. I, 4.ª ed., Coimbra, Coimbra Editora, 2007, pp. 547 ss. e anotação ao art. 35º da CRP em Jorge Miranda/ Rui Medeiros, *Constituição Portuguesa Anotada*, vol. I, 2.ª ed., Coimbra, Coimbra Editora, 2010, pp. 779 e ss.

[13] O RGPD estabeleceu não só vários direitos dos titulares dos dados pessoais como, ainda, a responsabilidade civil solidária dos responsáveis pelo seu tratamento em caso da sua violação, determinando, nomeadamente, uma presunção de culpa por parte dos lesantes. A este respeito, v. Tiago Branco da Costa, «A responsabilidade civil decorrente da violação do Regulamento Geral sobre a Proteção de Dados», in Alessandra Silveira/Joana Covelo de Abreu/Larissa Coelho, *UNIO E-Book INTEROP 2019*, Braga, Escola de Direito da Universidade do Minho/ JusGov, 2019, p. 68 ss., em especial, pp. 72 e 73-74.

por este instrumento jurídico – um Regulamento – que permite uma maior harmonização da legislação dos Estados-Membros[14].

Por outro lado, como veremos, este novo regime jurídico veio dar resposta às necessidades de protecção em caso de fluxos de dados transfronteiriços.

2. A proteção transfronteiriça concedida pelo RGPD

O Considerando (14) do RGPD explica que a protecção de dados pessoais *das pessoas singulares* prevista no seu regime deverá aplicar-se independentemente da sua nacionalidade ou do seu local de residência, excluindo-se o tratamento de dados pessoais efetuado por pessoas singulares no exercício de atividades exclusivamente pessoais ou domésticas – como a troca de correspondência ou a manutenção de listas de endereços, bem como a atividade das redes sociais (Considerando (18)), que se mantém ao abrigo da liberdade de cada um.

Assim, em primeiro lugar, o Considerando (22) determina a aplicação das regras do RGPD a qualquer tratamento de dados pessoais, efetuado no contexto das atividades de um estabelecimento, por parte de um responsável pelo tratamento de dados ou de um subcontratante situado na União, quer o tratamento em si tenha sido realizado na União, quer não[15]. Para tanto, não é necessário que a sede deste estabelecimento se encontre na UE, ou que o estabelecimento (sucursal, filial, ou qualquer outra forma jurídica) tenha personalidade jurídica, bastando que haja "o exercício efetivo e real de uma atividade com base numa instalação estável".

[14] Neste sentido, o Considerando (13) determina que "[a] fim de assegurar um nível coerente de proteção das pessoas singulares no conjunto da União e evitar que as divergências constituam um obstáculo à livre circulação de dados pessoais no mercado interno, é necessário um regulamento que garanta a segurança jurídica e a transparência aos operadores económicos, incluindo as micro, pequenas e médias empresas, que assegure às pessoas singulares de todos os Estados-Membros o mesmo nível de direitos suscetíveis de proteção judicial e imponha obrigações e responsabilidades iguais aos responsáveis pelo tratamento e aos seus subcontratantes, que assegure um controlo coerente do tratamento dos dados pessoais, sanções equivalentes em todos os Estados-Membros, bem como uma cooperação efetiva entre as autoridades de controlo dos diferentes Estados-Membros".

[15] Assim, independentemente da localização física dos servidores do prestador de serviços ou bens, o tratamento de dados pessoais de residentes na União Europeia encontra-se protegido pelas normas europeias. Neste sentido, Catarina Sarmento e Castro, «A jurisprudência do Tribunal de Justiça da União Europeia...», *cit.,* p. 1067.

Em segundo lugar, o Considerando (23) estabelece que o RGPD é aplicável às pessoas singulares que sejam titulares de dados pessoais que tenham sido objecto de tratamento, desde que estes titulares de dados pessoais se encontrem na UE, ainda que a entidade responsável pelo respectivo tratamento (ou o seu subcontratante) se encontre fora da União. Portanto, fundamental não é a nacionalidade da pessoa singular, nem a sua residência, mas o facto de se encontrar na UE e de, apesar de o responsável pelo tratamento se encontrar fora desta, as referidas atividades de tratamento de dados estarem relacionadas com a sua oferta de bens ou serviços a esses titulares, ainda que a título gratuito. Portanto, se um responsável se encontra fora da União Europeia, mas tem a intenção de fornecer bens ou serviços a pessoas singulares que se encontrem na União, o tratamento de dados pessoais que advenha destas relações estará sujeito às regras do RGPD.

Em terceiro lugar, o RGPD também alarga o seu círculo de protecção quanto ao tratamento de dados pessoais de pessoas singulares aos casos em que o responsável pelo seu tratamento visa analisar o comportamento dos titulares dos dados com vista a criar perfis[16], analisar, prever ou determinar as suas preferências e o seu comportamento, a fim de tomar decisões com base nos perfis elaborados.

Esta aplicação transfronteiriça do Regulamento visa evitar que as pessoas singulares que se encontram na UE se vejam privadas da proteçcão que lhes é conferida pelo RGPD, tanto nos casos em que contratam com entidades que se encontram na UE, mas cujo tratamento de dados é realizado fora desta, como nos casos em que tais entidades se encontram formalmente fora da UE, apesar de o bem ou serviço ser destinado a ser utilizado dentro desta; inclui, ainda, os casos em que os dados são recolhidos e tratados com vista a permitir a tais entidades tomar decisões com base nas informações coligidas e tratadas (nomeadamente, após a determinação de perfis, por exemplo, como vimos), visando o controlo do comportamento dos titulares do dados, desde que esse comportamento tenha lugar na União (art. 3º do RGPD).

[16] O artigo 4º, al. 4), do RGPD define "definição de perfis" como "qualquer forma de tratamento automatizado de dados pessoais que consista em utilizar esses dados pessoais para avaliar certos aspetos pessoais de uma pessoa singular, nomeadamente para analisar ou prever aspetos relacionados com o seu desempenho profissional, a sua situação económica, saúde, preferências pessoais, interesses, fiabilidade, comportamento, localização ou deslocações".

Apesar de esta aplicação ser uma novidade muito bem vista por parte dos cidadãos da UE, nem todos os Estados terceiros a terão visto com bons olhos, considerando-a uma ingerência na sua soberania. Contudo, a verdade é que vários destes Estados em breve se aperceberiam que a confiança dos consumidores depende, em boa parte, das garantias que lhes são oferecidas no que toca ao respeito pelos seus direitos fundamentais, nomeadamente no que toca ao tratamento dos seus dados pessoais e ao seu direito à privacidade. Assim, vimos surgir instrumentos de colaboração entre a UE e Estados terceiros, com vista a permitir a criação desta confiança.

Por exemplo, apesar de o RGPD proteger os cidadãos europeus ainda que os fornecedores de bens e serviços se encontrem fora da UE, esta protecção só funciona relativamente a tratamentos de dados relacionados com a prestação de bens ou serviços dentro da UE. Ou seja, caso um nacional português, tendo em vista uma visita que pretenda fazer aos Estados Unidos da América, entrasse em contacto com um restaurante em Nova Iorque e lhe fosse pedido o seu número de cartão de crédito a fim de assegurar a respectiva reserva, o tratamento destes seus dados pessoais por parte do restaurante não se encontrava abrangido pela protecção concedida pelo RGPD, já que a prestação se realizaria em solo norte-americano. Os seus dados pessoais e o seu número de cartão de crédito podiam, eventualmente, ser cedidos a outros restaurantes, ao abrigo de protocolos entre estes prestadores de bens e serviços, ainda que o seu titular não soubesse, nem tivesse consentido nisso.

Ora, a confiança dos agentes económicos e dos consumidores europeus poderia vir a sofrer com este decréscimo de proteçcão, inibindo-os de se aventurarem em solo estrangeiro; tal facto não prejudicaria só os consumidores europeus, mas o fluxo de pessoas, bens e serviços, bem como a economia dos países terceiros, assim excluídos.

Deste modo, os responsáveis por tratamento de dados (ou os seus subcontratantes) da UE só podem transferir dados para um país terceiro ou uma organização internacional se as condições estabelecidas no Capítulo V do RGPD forem respeitadas, incluindo as que se referem às transferências ulteriores de dados pessoais desse país terceiro ou organização internacional para outras entidades. Ou seja, o RGPD pretende assegurar "que não é comprometido o nível de proteção das pessoas singulares garantido pelo

presente regulamento" no caso de transferências transfronteiriças realizadas *por responsáveis por tratamentos de dados pessoais* (art. 44º do RGPD).

Para agilizar estas garantias, o art. 45º do RGPD prevê a possibilidade de a Comissão Europeia (CE) declarar que o regime jurídico de um determinado Estado apresenta um nível de protecção semelhante ao que vigora na UE, emitindo uma *decisão de adequação*. Graças às decisões de adequação, os dados pessoais podem circular livremente e em segurança a partir do Espaço Económico Europeu (ou seja, dos 27 Estados-Membros da UE, da Noruega, da Islândia e do Liechtenstein) para um país terceiro, sem estarem sujeitos a quaisquer outras condições ou autorizações. Desta forma, estas transferências de dados para um país terceiro – beneficiário de uma decisão de adequação – podem ser tratadas da mesma forma que as transmissões de dados no interior da UE[17].

O procedimento com vista à adoção de uma decisão de adequação inicia-se com uma proposta da CE, à qual se segue um parecer do Comité Europeu para a Proteção de Dados. Esta proposta terá de ser aprovada por representantes dos países da UE e só depois poderá ser adoptada pela CE. Neste momento, a CE adoptou decisões de adequação relativamente aos seguintes países e organizações: Andorra, Argentina, Canadá (organizações comerciais), Ilhas Faroé, Guernsey, Israel, Ilha de Man, Japão, Jersey, Nova Zelândia, República da Coreia, Suíça, Reino Unido (ao abrigo do RGPD), Estados Unidos da América (organizações comerciais que participam no Quadro de Privacidade de Dados UE-EUA, que iremos explorar em seguida) e Uruguai[18].

Nos termos do nº 2 do art. 45º, do RGPD, para avaliar a adequação do nível de proteção de um Estado terceiro, externo à UE, a Comissão considera, nomeadamente, os seguintes elementos:

> "a) O primado do Estado de direito, o respeito pelos direitos humanos e liberdades fundamentais, a legislação pertinente em vigor, tanto a geral como a setorial, nomeadamente em

[17] European Commission, *Questions and Answers: EU-US Data Privacy Framework* [em linha]. [Consult. 20/7/2023]. Disponível na Internet: https://ec.europa.eu/commission/presscorner/detail/en/qanda_23_3752.

[18] European Commission, *Adequacy decisions: How the UE determines if a non-EU country has an adequate level od data protection* [em linha]. [Consult. 20/7/2023]. Disponível na Internet: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

matéria de segurança pública, defesa, segurança nacional e direito penal, e respeitante ao acesso das autoridades públicas a dados pessoais, bem como a aplicação dessa legislação e das regras de proteção de dados, das regras profissionais e das medidas de segurança, incluindo as regras para a transferência ulterior de dados pessoais para outro país terceiro ou organização internacional, que são cumpridas nesse país ou por essa organização internacional, e a jurisprudência, bem como os direitos dos titulares dos dados efetivos e oponíveis, e vias de recurso administrativo e judicial para os titulares de dados cujos dados pessoais sejam objeto de transferência;

b) A existência e o efetivo funcionamento de uma ou mais autoridades de controlo independentes no país terceiro ou às quais esteja sujeita uma organização internacional, responsáveis por assegurar e impor o cumprimento das regras de proteção de dados, e dotadas de poderes coercitivos adequados para assistir e aconselhar os titulares dos dados no exercício dos seus direitos, e cooperar com as autoridades de controlo dos Estados-Membros; e

c) Os compromissos internacionais assumidos pelo país terceiro ou pela organização internacional em causa, ou outras obrigações decorrentes de convenções ou instrumentos juridicamente vinculativos, bem como da sua participação em sistemas multilaterais ou regionais, em especial em relação à proteção de dados pessoais".

Considerando todos estes factores, "a Comissão pode decidir, através de um ato de execução, que um país terceiro, um território ou um ou mais setores específicos de um país terceiro, ou uma organização internacional, garante um nível de proteção adequado" (art. 45º, nº 3, do RGPD). Esta decisão de adequação será reavaliada periodicamente (no mínimo de quatro em quatro anos), para garantir que o nível de protecção se mantém. Se não for o caso, a Comissão, "na medida do necessário, revoga, altera ou suspende a decisão referida (...) através de atos de execução, sem efeitos retroativos" (art. 45º, nº 5, do RGPD).

3. O Quadro de Privacidade dos Dados UE-EUA

3.1. Generalidades

A 25 de Março de 2022, a CE e os Estados Unidos da América (EUA) anunciaram que tinham chegado a acordo relativamente ao estabelecimento de um quadro transatlântico de privacidade de dados. Este acordo surgiu no seguimento de mais de um ano de negociações entre ambos, para dar resposta às preocupações levantadas pelo Tribunal de Justiça da EU (TJUE) no caso *Schrems II* de 16 de Julho de 2020[19].

Na sequência deste acordo, os Estados Unidos comprometeram-se a proceder a reformas estruturais da sua legislação para garantir a proteção da privacidade e das liberdades civis, nomeadamente, no que toca às actividades de vigilância no âmbito da segurança nacional, que deverão respeitar princípios como os da proporcionalidade e necessidade; para além disso, comprometeram-se a estabelecer um controlo rigoroso e independente destas actividades, de forma a garantir o efectivo cumprimento destes princípios, bem como a adoptar medidas de remédio em caso da sua violação. A declaração conjunta da CE e dos EUA deixa claro que este Quadro pretende garantir o fluxo de dados entre os Estados-Membros da UE e os EUA, sendo visto como fundamental para proteger os direitos dos cidadãos e permitir o comércio transatlântico em todos os sectores da economia, nomeadamente, promovendo uma economia digital inclusiva, em que todas as pessoas e empresas de todas as dimensões possam participar, permitindo o desenvolvimento económico de todas as partes envolvidas[20].

---

[19] Ac. TJUE (Grande Secção) 16/7/2020, proc. nº C-311/18 *Facebook Ireland e Schrems v. Data Protection Commissioner (Schrems II)*, [Consult. 21/07/2023]. Disponível na Intranet: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:62018CJ0311. Já anteriormente, no caso *Schrems I* (TJUE, *Maximilian Schrems v. Facebook Ireland Limited*, Case C-498/16, de 25 de janeiro de 2018), o TJUE tinha considerado que o contrato que liga o utilizador do Facebook a esta rede social é um contrato de consumo internacional. Anabela Susana de Sousa Gonçalves, «O caso Schrems contra Facebook e o contrato de Consumo Internacional», in Isabel Celeste M. Fonseca [et al.], *Desafios do Direito no Século XXI: uma Reflexão Luso-Brasileira sob o Signo Interdisciplina,* [S. l.], Escola de Direito da Universidade do Minho/JusGov, 2019, p. 39.

[20] European Commission, *European Commission and United States Joint Statement on Trans-Atlantic Data Privacy Framework* [em linha], 25 de Março de 2022. [Consult. 19/7/2023]. Disponível na Intranet: https://ec.europa.eu/commission/presscorner/detail/pt/ip_22_2087.

A 10 de Julho de 2023, a CE adoptou a Decisão de Adequação relativamente ao Quadro de Privacidade de Dados UE-EUA[21]. A decisão conclui que os Estados Unidos asseguram um nível de proteção adequado — comparável ao da União Europeia — dos dados pessoais transferidos da UE para empresas dos EUA ao abrigo do novo quadro. Com base na nova decisão de adequação, os dados pessoais podem circular em segurança da UE para as empresas dos EUA que participam no quadro, sem necessidade de estabelecer salvaguardas adicionais em matéria de proteção de dados[22].

A Presidente da CE, Ursula von der Leyen, afirmou, a este respeito:

> "The new EU-U.S. Data Privacy Framework will ensure safe data flows for Europeans and bring legal certainty to companies on both sides of the Atlantic. Following the agreement in principle I reached with President Biden last year, the US has implemented unprecedented commitments to establish the new framework. Today we take an important step to provide trust to citizens that their data is safe, to deepen our economic ties between the EU and the US, and at the same time to reaffirm our shared values. It shows that by working together, we can address the most complex issues"[23].

Exploremos, agora, este documento.

3.2. A Decisão de Adequação relativamente ao Quadro de Privacidade de Dados UE-EUA

No texto da Decisão de Adequação, a CE começa por explicar que é necessário garantir que os países terceiros beneficiários da referida decisão

---

[21] European Commission, *Commission Implementing Decision of 10.7.2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework* [em linha]. 10 de Julho de 2023. [Consult. 21/07/2023]. Disponível na Intranet: https://commission.europa.eu/system/files/2023-07/Adequacy%20decision%20EU-US%20Data%20Privacy%20Framework_en.pdf.

[22] European Commission, *Data Protection: European Commission adopts new adequacy decision for safe and trusted EU-US data flows* [em linha], 10 de Julho de 2023. [Consult. 19/7/2023]. Disponível na Intranet: https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3721.

[23] *Idem.*

possuem um nível de protecção de dados pessoais "essencialmente equivalente" àquele que existe na EU, considerando não só os normativos aplicáveis (como o RGPD) como a jurisprudência do Tribunal de Justiça da União Europeia (Considerando (3))[24]. Tal não significa que as regras do RGPD devam encontrar-se reproduzidas no regime jurídico deste país terceiro, mas apenas que, considerando a globalidade do seu ordenamento jurídico, as medidas adoptadas por este país garantem um nível de protecção efectivo e adequado no que toca aos direitos à privacidade, possuindo mecanismos de garantia e de supervisão quanto ao seu respeito. Por exemplo, a CE deverá assegurar-se que o referido país terceiro possui legislação capaz de garantir que as interferências relativas aos direitos fundamentais de titulares de dados pessoais oriundos da UE, ainda que legítimas – por motivos de segurança nacional, e.g. –, sejam sujeitas a controlo legal e protecção efectiva (Considerando (4)).

O Considerando (5) explica qual é o nível de adequação considerado adequado pelo Tribunal de Justiça da UE (TJUE), dando conta do caso C-311/18, *Data Protection Commissioner versus Facebook Ireland Limited and Maximillian Schrems (Schrems II)*. Neste caso, o TJUE invalidou a decisão anterior da CE no sentido de considerar adequado o anterior quadro transatlântico de fluxo de dados entre a UE e os EUA (o chamado *EU-U.S. Privacy Shield*) com vários fundamentos: em primeiro lugar, entendeu que as limitações à protecção de dados pessoais decorrentes da lei interna dos EUA, no que tocava ao acesso e uso dos dados pessoais provenientes da UE por parte das entidades públicas devido a finalidades de segurança nacional, não cumpria os requisitos de necessidade e proporcionalidade exigidos à luz do nível de protecção garantido na UE; em segundo lugar, que a lei interna dos EUA não previa fundamentos legais para que os lesados pudessem recorrer de tais limitações ou ingerências nos seus direitos perante uma entidade que oferecesse garantias semelhantes às determinadas no art. 47º da Carta dos Direitos Fundamentais da União Europeia[25]. Esta norma prevê um direito à

[24] European Commission, *Commission Implementing Decision of 10.7.2023 pursuant to Regulation (EU) 2016/679...*, pp. 1 e 2.

[25] Carta dos Direitos Fundamentais da União Europeia, *Jornal Oficial da União Europeia* C 202/403, de 7/06/2016, p. 403. [Consult. 15/07/2023]. Disponível na Intranet: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:12016P/TXT.

ação e a um tribunal independente e imparcial por parte de todas as pessoas cujos direitos e liberdades garantidos pelo Direito da União Europeia tenham sido violados.

Assim, tendo em consideração o decidido por parte do TJUE, a CE entrou em negociações com os EUA a fim de tornar possível uma nova decisão de adequação, desde que a lei interna dos EUA suprisse estas faltas. No seguimento destas negociações, em 7 de Outubro de 2022, os EUA adoptaram a "Executive Order 14086 'Enhancing Safeguards for US Signals Intelligence Activities' (EO 14086)", complementada pela *Regulation on the Data Protection Review Court* a cargo do *U.S. Attorney General* ("AG Regulation"). Paralelamente, o quadro legal aplicável às entidades comerciais que processavam dados pessoais transferidos da UE ao abrigo da decisão de adequação ("EU-U.S. Data Privacy Framework") foi também actualizado (Considerando (6)). Após a análise de todas estas alterações na lei interna dos EUA, a CE concluiu que os EUA garantiam um nível adequado de protecção relativamente aos dados pessoais transferidos da UE para os EUA, ao abrigo do Quadro de Privacidade de Dados UE-EUA, por parte de um responsável pelo tratamento de dados da UE ou pelo seu subcontratante, tendo como destinatários organizações certificadas nos EUA (Considerando (7)).

Isto significa que quaisquer fluxos de dados pessoais entre um responsável pelo tratamento de dados da UE ou pelo seu subcontratante e as organizações certificadas nos EUA ao abrigo do Quadro de Privacidade de Dados UE-EUA não necessitam de uma autorização adicional; naturalmente, tal não invalida a protecção que lhes é concedida ao abrigo do regime geral do RGPD, nomeadamente no seu artigo 3º, já referido *supra*.

3.3. O Quadro de Privacidade de Dados UE-EUA

O Quadro de Privacidade de Dados UE-EUA baseia-se num sistema de certificação. As entidades norte-americanas que pretendam ser certificadas ao abrigo deste quadro para beneficiar do regime referido no ponto anterior, devem comprometer-se a cumprir os "EU-U.S. Data Privacy Framework Principles", bem como os Princípios Suplementares emitidos pelo *Department of Commerce* (DoC) dos EUA e incluídos no Anexo I da decisão de

adequação[26]. A sua adesão a estes Princípios tem de ser renovada anualmente (Considerando (9)).

O Considerando (11) explica que os Princípios (incluindo nesta referência não só os "EU-U.S. Data Privacy Framework Principles" como também os Princípios Suplementares) definem dados ou informação pessoal nos mesmos termos do nosso RGPD (como "data about an identified or identifiable individual that are within the scope of the GDPR received by an organization in the United States from the EU, and recorded in any form"); o mesmo sucede no que toca à noção de "tratamento de dados pessoais" (que definem como "any operation or set of operations which is performed upon personal data, whether or not by automated means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure or dissemination and erasure or destruction").

Como garantia adicional, o Considerando (12) dá conta de que o Quadro de Privacidade de Dados UE-EUA se aplica a organizações dos EUA que se qualifiquem como responsáveis por tratamento de dados (os chamados "controllers", que se definem como "a person or organisation which, alone or jointly with others, determines the purposes and means of the processing of personal data") ou subcontratantes ("agentes acting on behalf of a controller"). Os subcontratantes dos EUA devem estar contratualmente obrigados a atuar apenas sob instruções do responsável pelo tratamento da UE e a prestar-lhe assistência, caso os titulares dos dados exerçam os seus direitos ao abrigo dos princípios. Caso um subcontratante dos EUA venha, por seu lado, também a subcontratar as operações de tratamento de dados com outra entidade, também sobre esta entidade deverão recair as mesmas obrigações, devidamente estabelecidas através de contrato, garantindo-se, assim, o mesmo nível de protecção estabelecido pelos Princípios[27].

---

[26] European Commission, *Commission Implementing Decision of 10.7.2023 pursuant to Regulation (EU) 2016/679...*, pp. 66 e ss.

[27] *Idem*, p. 4.

Os Princípios em causa são os seguintes:

a) *Princípio da Integridade dos Dados e da Limitação da Finalidade ("Data Integrity and Purpose Limitation Principle")*

Tal como sucede no art. 5º, nº 1, al. b), do RGPD, uma organização só pode proceder ao tratamento de dados de acordo com a finalidade para a qual estes foram recolhidos, a não ser que o titular dos dados o autorize subsequentemente ou tal processamento não seja incompatível com a finalidade para a qual foram recolhidos originalmente (Considerando (14)).

Por outro lado, os dados devem ser exactos, o que significa que devem ser actualizados, se necessário. Além disso, devem ser adequados em relação às finalidades para as quais foram recolhidos, ou seja, não poderão ser excessivos, nem conservados para além do período necessário para se atingirem tais finalidades (Considerandos (20) e (21)). No entanto, há excepções a esta regra temporal, ainda que os dados continuem sujeitos às salvaguardas previstas nos Princípios: para finalidades de arquivo de interesse público, jornalismo, literatura e arte, investigação científica e histórica e análise estatística (Considerando (22)).

b) *Princípio da Escolha ("Choice Principle")*

Ainda que o novo tratamento (ou a exposição dos dados a terceiros) seja compatível com a finalidade para a qual os dados foram recolhidos (e em relação à qual o seu titular deu já o respectivo consentimento ao tempo da referida recolha), a organização é obrigada a conceder-lhe a possibilidade de objectar a um novo tratamento, ou seja, de escolher/optar por recusar o referido tratamento ("opt-out") através de um mecanismo claro, visível e facilmente disponível. Este princípio não substitui a proibição expressa de realizar um tratamento incompatível com a referida finalidade (Considerando (15)).

Ainda de acordo com o Princípio da Escolha, os dados sensíveis estão protegidos por salvaguardas adicionais (Considerando (16)). Tais dados são definidos como "personal data specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade

union membership, information on the sex life of the individual or any other information received from a third party that is identified and treated by that party as sensitive". Como vemos, esta definição vai de encontro à do RGPD, incluindo-se aqui os dados relativos à orientação sexual, dados genéticos e dados biométricos (Considerando (17)). Em regra, para que uma organização possa proceder ao tratamento de dados sensíveis para outras finalidades que não aquelas para as quais estes foram recolhidos (ou para que os possa expor a terceiros), necessita do consentimento *expresso* ("opt-in") do seu titular (Considerando (18)). Excepcionalmente, e à semelhança do que sucede com o RGPD, tal não será necessário: por exemplo, caso o processamento destes dados sensíveis seja do interesse vital de uma pessoa; caso seja necessário para intentar acções judiciais; caso seja necessário para a prestação de cuidados médicos ou de diagnóstico (Considerando (19)).

c) *Princípio da Segurança ("Security Principle")*

Os dados pessoais também devem ser processados de forma a garantir-se a sua segurança, nomeadamente contra processamentos ilegais ou não autorizados, perdas acidentais, destruição ou outro tipo de danos. Assim, os responsáveis pelo tratamento de dados e os seus subcontratantes devem adoptar todas as medidas apropriadas para garantir a sua segurança, considerando o desenvolvimento da técnica, a natureza dos dados, os custos das medidas em causa e os riscos para os direitos dos titulares envolvidos, à semelhança do determinado pelo art. 32º do RGPD (Considerandos (23) e (24).

d) *Princípio da Notificação ("Notice Principle")*

Tal como sucede com o princípio da transparência do RGPD, os *EU-U.S. Data Privacy Framework Principles* também exigem que os titulares dos dados sejam informados das principais características do processamento dos seus dados pessoais: a participação da organização no *Data Privacy Framework*; o tipo de dados recolhidos; a finalidade do tratamento dos dados; o tipo ou a identidade dos terceiros aos quais os dados pessoais podem ser comunicados e as finalidades desse tratamento; os seus direitos individuais; a forma de contactar a organização e as vias de recurso disponíveis (Considerandos (25) e (26)).

Para que estas informações sejam efectivamente conhecidas dos titulares dos dados, a linguagem em que são transmitidas tem de ser clara e acessível; estas informações devem ser prestadas quando se pede aos titulares dos dados que os forneçam pela primeira vez ou logo que possível após essa data, mas nunca depois de os dados serem utilizados para outra finalidade, ainda que compatível com aquela para que foram recolhidos, ou depois de serem divulgados a terceiros (Considerando (27)).

Para garantir a possibilidade de conhecimento por parte dos interessados, as políticas de privacidade destas organizações – que devem refletir os Princípios a que aderiram e que justifica a sua certificação como tal – devem estar disponíveis ao público, devendo estas organizações, ainda, disponibilizar *links* para o *website* do *Department of Commerce* (DoC) dos EUA, que conterá mais pormenores sobre certificação, os direitos dos titulares dos dados e os mecanismos de recurso disponíveis, a Lista das organizações participantes no *Data Privacy Framework* e o *website* de um prestador alternativo adequado de serviços de resolução de litígios (Considerando (28)).

e) *O Princípio do Acesso (Access Principle): direitos individuais dos titulares dos dados pessoais*

Aos titulares de dados pessoais são reconhecidos direitos individuais que podem ser defendidos perante uma entidade supervisora independente, através de mecanismos previstos contra o responsável pelo tratamento de dados ou o seu subcontratante: o direito de aceder aos dados, o direito de se opor ao seu tratamento; o direito de rectificar ou apagar os dados (Considerando (29)). Estes direitos baseiam-se no Princípio do Acesso:

aa) Os titulares dos dados têm o direito de exigir de qualquer organização – sem necessidade de justificação alguma – que confirme se está a processar dados pessoais seus; que tipo de dados são esses; qual a finalidade do processamento e a quem tais dados são revelados. As organizações são obrigadas a responder dentro de um prazo razoável, embora possam exigir o pagamento de uma taxa (que não poderá ser excessiva), caso estes pedidos de esclarecimento se tornem repetitivos e, por isso, manifestamente excessivos. Poderá, também, estabelecer um número-limite de vezes em que o mesmo

titular poderá requerer o acesso a estas informações dentro de um determinado prazo, desde que tal limite seja razoável (Considerando (30)).

Tal como sucede no direito da UE, este direito de acesso pode ser limitado em situações excepcionais: quando os direitos legítimos de terceiros possam ser violados; quando os encargos ou a despesa de facultar o acesso forem desproporcionados em relação aos riscos para a privacidade do indivíduo nas circunstâncias do caso (embora tais despesas e encargos não sejam factores de controlo para determinar se o acesso é razoável ou não); na medida em que a divulgação seja suscetível de interferir com a salvaguarda de interesses públicos importantes (como a segurança nacional, a segurança pública ou a defesa); quando se relacionam com informações comerciais confidenciais; ou quando a informação é tratada exclusivamente para fins de investigação ou fins estatísticos. De todo o modo, ainda que seja aplicável alguma destas excepções, cabe à organização justificar esta limitação ao direito de acesso dos titulares dos dados e de provar que estas circunstâncias se verificam, devendo apenas excluir a informação que se inclua nestas e divulgar a restante (Considerando (31)).

bb) Os titulares de dados pessoais têm o direito de obter a rectificação ou alteração de dados inexactos e de obter a eliminação daqueles que tenham sido tratados em violação dos princípios. Além disso, como já vimos, têm o direito de se opor ao tratamento dos seus dados para fins materialmente diferentes (ainda que compatíveis) com as finalidades para as quais os dados foram recolhidos, bem como à sua divulgação a terceiros. Caso os seus dados pessoais sejam utilizados para fins de *marketing* direto, têm, ainda, o direito geral de se oporem ao tratamento a qualquer momento (Considerando (32)).

cc) Apesar de os Princípios não preverem nenhuma regra relativamente ao processamento automatizado de dados com a finalidade de se tomar decisões relativas aos titulares de dados pessoais, sendo estes recolhidos no seio da UE, tais decisões serão tomadas por um responsável de tratamento de dados pessoais da UE, que se encontra, portanto, sob a alçada do RGPD. Esta situação mantém-se, ainda que tais dados sejam transferidos para os EUA pelo responsável pelo seu tratamento da UE (ou pelo seu subcontratante da UE), actuando a organização dos EUA como subcontratante destes (Considerando

(32)). De todo o modo, foi feita uma análise à legislação interna dos EUA que concluiu que esta possui vários mecanismos que protegem os titulares dos dados em várias situações como estas, nomeadamente as que dizem respeito a crédito ao consumo, crédito hipotecário, emprego, habitação e seguros, etc.[28]. Assim, considerou-se que, na hipótese improvável de a decisão vir a ser tomada pela própria organização norte-americana, a protecção oferecida pelo sistema dos EUA é similar à oferecida pelo sistema da EU (Considerando (36)).

f) *Princípio da Responsabilidade pela Transferência Subsequente (Accountability for Onward Transfer Principle)*

Este princípio visa impedir que as regras estabelecidas no Quadro de Privacidade de Dados UE-EUA sejam defraudadas por via da transferência das operações de tratamento de dados para terceiros não aderentes aos Princípios (estejam estes localizados dentro ou fora dos EUA). Uma transferência subsequente só poderá realizar-se no caso de finalidades específicas e limitadas e apenas com base num contrato entre a organização dos EUA (que recebeu os dados da UE) e a entidade terceira, contrato, este, que tem, obrigatoriamente, de prever o mesmo nível de protecção garantido pelos Princípios. Ou seja, esta entidade terceira terá de respeitar, ela própria, os Princípios da Integridade dos Dados e da Limitação da Finalidade, o Princípio da Escolha, o Princípio da Notificação, nos termos já explorados (Considerandos (37) a (40). O mesmo processo deverá repetir-se, caso esta entidade venha a subcontratar as suas funções em outra entidade terceira (Considerando (41)).

[28] O Considerando (35) determina, a este respeito o seguinte: "In any event, in areas where companies most likely resort to the automated processing of personal data to take decisions affecting the individual (e.g. credit lending, mortgage offers, employment, housing and insurance), U.S. law offers specific protections against adverse decisions. These acts typically provide that individuals have the right to be informed of the specific reasons underlying the decision (e.g. the rejection of a credit), to dispute incomplete or inaccurate information (as well as reliance on unlawful factors), and to seek redress. In the area of consumer credit, the Fair Credit Reporting Act (FCRA) and Equal Credit Opportunity Act (ECOA) contain safeguards that provide consumers with some form of a right to explanation and a right to contest the decision. These Acts are relevant in a wide range of areas, including credit, employment, housing and insurance. In addition, certain anti-discrimination laws, such as Title VII of the Civil Rights Act and the Fair Housing Act, provide individuals with protections with respect to models used in automated decision-making that could lead to discrimination on the basis of certain characteristics, and grant individuals rights to challenge such decisions, including automated ones". European Commission, *Commission Implementing Decision of 10.7.2023 pursuant to Regulation (EU) 2016/679...,* p. 9.

É interessante notar que o contrato em questão deve prever a obrigação de a entidade terceira notificar a organização sujeita ao Quadro de Privacidade dos Dados UE-EUA, caso deixe de respeitar as suas obrigações, momento a partir do qual deverá cessar as operações de tratamento de dados e resolver a situação de forma adequada. Caso se verifiquem problemas de incumprimento numa cadeia de subcontratações de tratamento de dados, a organização que actue como responsável do seu tratamento responderá civilmente, tal como determina o Princípio do Recurso, da Execução e da Responsabilidade, a menos que prove não ser responsável pelo evento causador dos danos (Considerandos (42) e (43)).

g) *Princípio do Recurso, da Execução e da Responsabilidade (Recourse, Enforcement and Liability Principle)*

Este princípio diz respeito ao Princípio da Responsabilização ("accountability"), que determina que as entidades que processem dados devem criar medidas técnicas e organizacionais apropriadas para garantir o cumprimento das suas obrigações relativamente à protecção dos dados a seu cargo. Devem, ainda, estar em condições de provar este cumprimento às competentes entidades supervisoras. Ou seja, assim, que uma entidade decide aderir voluntariamente ao Quadro de Privacidade dos Dados UE-EUA através da respectiva certificação, é obrigada a cumprir os seus Princípios de forma efectiva. Pode fazê-lo através de procedimentos internos (assegurando a devida formação aos seus funcionários, por exemplo; através de auditorias internas que verifiquem periodicamente o cumprimento das suas obrigações) ou através de procedimentos externos (como auditorias externas, controlos aleatórios, uso de ferramentas tecnológicas, etc.). Estas práticas devem ser mantidas num registo, para que possam ser disponibilizadas às competentes entidades supervisoras no contexto de uma investigação ou de uma queixa de não cumprimento perante um organismo independente de resolução de litígios ou a competente autoridade de execução (Considerandos (44) a (46)).

3.4. Administração, supervisão e aplicação do Quadro de Privacidade dos Dados UE-EUA

Finalmente, resta-nos explorar de que forma é que todos este princípios e normas são implementados na prática.

A entidade responsável pela supervisão da sua efectiva implementação é o *Departament of Commerce* (DoC) dos EUA (Considerandos (47)). É este departamento que trata da certificação e re-certificação (anual) das organizações que pretendem aderir (ou conservar a sua adesão) voluntariamente aos Princípios do Quadro de Privacidade, mantendo a lista actualizada das entidades certificadas no seu *website* (Considerandos (48) a (52)). É também o DoC que possui competência para realizar vistorias aleatórias às organizações em causa, a fim de determinar se, efectivamente, cumprem as obrigações que para elas advêm dos Princípios do Quadro de Privacidade (Considerando (53)), e que tem competência para excluir tais organizações da lista, caso o incumprimento destas obrigações seja recorrente (nos termos do procedimento descrito nos Considerandos (54) a (55)). Caso assim seja, estas organizações terão de devolver ou apagar os dados que receberam ao abrigo do Quadro de Privacidade. O mesmo se diga quanto a organizações que afirmem falsamente actuar sob o Quadro de Privacidade (por exemplo, porque falharam os prazos ou não cumpriram os requisitos dos requerimentos de certificação ou de re-certificação, etc.). O DoC tanto pode actuar *ex officio,* como na sequência de queixas que lhe tenham sido apresentadas (nos termos dos Considerandos (56) e ss.).

Para além do DoC, ainda temos outra entidade com competências neste âmbito: a *U.S. Federal Trade Commission* (FTC). A FTC é uma autoridade independente, composta por cinco comissários nomeados pelo Presidente, sob e com o consentimento do Senado. Os comissários exercem as suas funções em exclusividade por um período de sete anos. Estas incluem investigar o cumprimento dos Princípios, investigar falsas alegações de adesão aos Princípios, etc. Caso a FTC encontre situações anómalas, garantirá o cumprimento do Quadro de Privacidade de Dados através do recurso a ordens administrativas ou de tribunais federais, ou mesmo arbitrando acordos, estabelecendo injunções preliminares ou permanentes, cujo cumprimento também controlará. Caso estas medidas não sejam cumpridas, a FTC pode solicitar sanções civis, nomeadamente com fundamento nos danos causados ilegalmente; além disso,

a FTC mantém uma lista *online* das organizações sujeitas a estas medidas ou a processos em tribunal (Considerandos (58) a (61)).

Como vemos, os titulares de dados pessoais que vejam os seus direitos violados podem recorrer a vários mecanismos à sua escolha, tanto administrativos como judiciais.

A primeira hipótese é a de recorrer directamente contra a própria organização dos EUA que procede às operações de tratamento dos seus dados, através de queixa, já que estas organizações, a fim de serem certificadas, são obrigadas a prever mecanismos de recurso independentes, que efectivamente investiguem e apresentem soluções sem qualquer custo para o titular dos dados. Estes mecanismos independentes tanto podem estar estabelecidos nos EUA como na UEE; em alternativa, as organizações podem recorrer a entidades independentes de resolução alternativa de litígios. De uma forma ou de outra, as organizações são obrigadas a disponibilizar um ponto de contacto (dentro ou fora da sua organização) para o qual as queixas serão dirigidas, bem como o corpo independente de resolução alternativa de litígios. A organização é obrigada a responder às queixas no prazo de 45 dias (Considerando (69)).

No entanto, os titulares de dados pessoais, em vez de se dirigirem à organização, podem recorrer directamente à entidade independente designada por esta para a resolução alternativa de litígios, ou à *Data Protection Authority* nacional em causa, ao DoC ou até à FTC. Se todas estas queixas não conduzirem a uma resolução do problema, como *ultima ratio*, os titulares dos dados podem ainda recorrer à arbitragem vinculativa prevista no Anexo I dos *EU-U.S. Data Privacy Framework Principles Issued by the U.S. Department Of Commerce*[29] (Considerandos (68), (73) a (87)).

4. Notas conclusivas

Como vimos, apesar de os EUA não possuírem uma regulamentação que replique o nosso RGPD, possuem vários mecanismos que garantem a protecção dos cidadãos europeus cujos dados pessoais sejam transferidos

[29] European Commission, *Commission Implementing Decision of 10.7.2023 pursuant to Regulation (EU) 2016/679...*, p. 95.

para um subcontratante nos EUA por parte do responsável pelo tratamento de dados pessoais na UE, que será a pessoa que os recolheu.

Para além disso, como vimos, desde que as organizações dos EUA que procedam ao tratamento de dados pessoais se encontrem certificadas (e, por isso, colocadas na lista do Quadro de Privacidade de Dados UE-EUA), têm de respeitar princípios semelhantes aos que vigoram na UE, havendo entidades competentes previstas na legislação nacional norte-americana para lidar com o seu incumprimento e garantir o devido ressarcimento em caso de danos e demais medidas necessárias e adequadas à situação em concreto.

Assim, a Decisão de Conformidade da CE determina no seu artigo 1º que, para os efeitos do artigo 45º do RGPD, os EUA asseguram um nível adequado de protecção dos dados pessoais que sejam transferidos da UE para as organizações que se encontrem elencadas na lista do Quadro de Privacidade de Dados que é mantido e tornado público pelo DoC dos EUA.

O problema estará, cremos, nos casos em que seja o próprio titular de dados pessoais a ceder os seus dados a organizações norte-americanas, quando estas não se encontrem certificadas, nem se tenham comprometido a respeitar os referidos princípios. Ainda que a recolha dos dados tenha sido efectuada na UE (pois, nos termos do art. 4º, al. 2), do RGPD, a simples recolha de dados já é considerada "tratamento de dados"), se o responsável pelo tratamento de dados possuir a sua sede ou estabelecimento fora da UE e as actividades de tratamento estiverem relacionadas com a oferta de bens ou serviços fora da UE, estaremos fora do âmbito de aplicação territorial do RGPD (cfr. o seu artigo 3º) e não se tratará de um caso de transferência de dados pessoais ao abrigo dos seus artigos 44º e ss. O mesmo se diga caso a recolha for feita já nos EUA, onde é de aplicar a lei norte-americana *tout-court*...

É caso para dizer: "em Roma, sê romano".