2025/2574

23.12.2025

DECISÃO DE EXECUÇÃO (UE) 2025/2574 DA COMISSÃO

de 19 de dezembro de 2025

que altera a Decisão de Execução (UE) 2021/1772 da Comissão nos termos do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho sobre a adequação do nível de proteção dos dados pessoais assegurado pelo Reino Unido

[notificada com o número C(2025) 8771]

(Texto relevante para efeitos do EEE)

A COMISSÃO EUROPEIA,

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

Tendo em conta o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados) ([1]), nomeadamente o artigo 45.º, n.º 3,

Considerando o seguinte:

1. INTRODUÇÃO

(1) A Decisão de Execução (UE) 2021/1772 da Comissão ([2]) conclui que, para efeitos do artigo 45.º do Regulamento (UE) 2016/679, o Reino Unido assegura um nível adequado de proteção dos dados pessoais transferidos da União Europeia para o Reino Unido no âmbito desse regulamento ([3]).

(2) Ao adotar a Decisão de Execução (UE) 2021/1772, a Comissão teve em conta que, após o termo do período de transição previsto no Acordo sobre a Saída do Reino Unido da Grã-Bretanha e da Irlanda do Norte da União Europeia e da Comunidade Europeia da Energia Atómica ([4]) e uma vez que a disposição provisória prevista no artigo 782.º do Acordo de Comércio e Cooperação entre a União Europeia e a Comunidade Europeia da Energia Atómica, por um lado, e o Reino Unido da Grã-Bretanha e da Irlanda do Norte, por outro ([5]), deixasse de ser aplicável, o Reino Unido adotaria, aplicaria e faria cumprir um novo regime de proteção diferente do que estava em vigor quando estava vinculado pelo direito da União.

(3) Dado que tal pode ter envolvido alterações do quadro de proteção de dados avaliado na Decisão de Execução (UE) 2021/1772 ou outros desenvolvimentos pertinentes, considerou-se adequado prever que essa decisão seria aplicável por um período de quatro anos a partir da sua entrada em vigor. Por conseguinte, a caducidade da Decisão de Execução (UE) 2021/1772 estava prevista para 27 de junho de 2025, a menos que fosse prorrogada nos termos do procedimento referido no artigo 93.º, n.º 2, do Regulamento (UE) 2016/679.

([1]) JO L 119 de 4.5.2016, p. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj.

([2]) Decisão de Execução (UE) 2021/1772 da Comissão, de 28 de junho de 2021, nos termos do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho sobre a adequação do nível de proteção dos dados pessoais assegurado pelo Reino Unido (JO L 360 de 11.10.2021, p. 1, ELI: http://data.europa.eu/eli/dec_impl/2021/1772/oj).

([3]) Ver artigo 1.º, n.º 1, da Decisão de Execução (UE) 2021/1772. Segundo o artigo 1.º, n.º 2, dessa decisão, esta não abrange os dados pessoais transferidos para os efeitos de controlo da imigração do Reino Unido ou que, de outro modo, sejam abrangidos pelo âmbito da isenção de determinados direitos dos titulares de dados, para efeitos de manutenção de um controlo efetivo da imigração, nos termos do *schedule* 2, n.º 4, ponto 1, da *Data Protection Act 2018* [não traduzida para português] do Reino Unido.

([4]) JO C 384I de 12.11.2019, p. 1.

([5]) JO L 149 de 30.4.2021, p. 10, ELI: http://data.europa.eu/eli/agree_internation/2021/689(1)/oj.

(4) Para decidir sobre uma possível prorrogação da Decisão de Execução (UE) 2021/1772, a Comissão deve avaliar se a conclusão de que o Reino Unido assegura um nível adequado de proteção continua a justificar-se de facto e de direito à luz dos desenvolvimentos que ocorreram desde a adoção da Decisão de Execução (UE) 2021/1772 no que diz respeito aos elementos enumerados no artigo 45.º, n.º 2, do Regulamento (UE) 2016/679.

(5) Especificamente a este respeito, em 23 de outubro de 2024, o Governo do Reino Unido apresentou no Parlamento o *Data (Use and Access) Bill* [Projeto de lei relativo ao acesso aos dados e à sua utilização] ([6]), que propõe alterações ao *General Data Protection Regulation* [Regulamento Geral sobre a Proteção de Dados] do Reino Unido (RGPD do reino Unido) e a *Data Protection Act 2018* [Lei de 2018 relativa à Proteção de Dados] (DPA 2018), os quais são avaliados na Decisão de Execução (UE) 2021/1772. Em 24 de junho de 2025, a Comissão adotou a Decisão de Execução (UE) 2025/1226 ([7]), a qual prorrogou a validade da Decisão de Execução (UE) 2021/1772 por um período de seis meses, até 27 de dezembro de 2025. Esta prorrogação técnica, limitada no tempo, permitiu à Comissão finalizar a sua avaliação do nível adequado de proteção dos dados pessoais fornecido pelo Reino Unido com base num quadro jurídico estável, isto é, na sequência da conclusão do processo legislativo pertinente ([8]).

(6) A Comissão controlou, de forma continuada, desde a adoção da Decisão de Execução (UE) 2021/1772, os desenvolvimentos pertinentes no Reino Unido ([9]). Em conformidade com o considerando 281 da Decisão de Execução (UE) 2021/1772, foi prestada especial atenção à aplicação, na prática, das regras do Reino Unido em matéria de transferências de dados pessoais para países terceiros e ao impacto que podem ter no nível de proteção oferecido aos dados transferidos ao abrigo da Decisão de Execução (UE) 2021/1772, à eficácia do exercício dos direitos das pessoas, incluindo qualquer desenvolvimento pertinente da legislação e das práticas relativas às exceções ou restrições a esses direitos (nomeadamente a que diz respeito à manutenção de um controlo efetivo da imigração); bem como à conformidade com as restrições e as garantias em matéria de acesso governamental. Entre outros elementos, o controlo da Comissão baseou-se nos desenvolvimentos da jurisprudência e na supervisão do Gabinete do Comissário para a Informação (ICO, do inglês *Information Commissioner's Office*) e de outros organismos independentes.

(7) Com base na apreciação destes desenvolvimentos, incluindo as alterações ao RGPD do Reino Unido e à DPA 2018 introduzidas pela *Data (Use and Access) Act*, a Comissão conclui que o Reino Unido continua a assegurar um nível de proteção adequado dos dados pessoais transferidos no âmbito do Regulamento (UE) 2016/679 da União Europeia para o Reino Unido.

(8) A Comissão conclui ainda que, à luz das alterações às disposições pertinentes do direito do Reino Unido ([10]), deixou de se justificar a exclusão dos dados pessoais transferidos para efeitos de controlo da imigração do Reino Unido ou que, de outro modo, sejam abrangidos pelo âmbito da isenção de determinados direitos dos titulares de dados, para efeitos de manutenção de um controlo efetivo da imigração (a «isenção relativa à imigração»), nos termos do *schedule* 2, n.º 4, ponto 1, da *Data Protection Act* do Reino Unido do âmbito de aplicação da Decisão de Execução (UE) 2021/1772, como explicado no considerando 37 da presente decisão.

([6]) Disponível na seguinte ligação: https://bills.parliament.uk/bills/3825/news.

([7]) Decisão de Execução (UE) 2025/1226 da Comissão, de 24 de junho de 2025, que altera a Decisão de Execução (UE) 2021/1772 nos termos do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho sobre a adequação do nível de proteção dos dados pessoais assegurado pelo Reino Unido (JO L, 2025/1226, 26.6.2025, ELI: http://data.europa.eu/eli/dec_impl/2025/1226/oj).

([8]) A *Data (Use and Access) Act* [Lei relativa ao acesso aos dados e à sua utilização] recebeu a aprovação real em 19 de junho de 2025.

([9]) Artigo 45.º, n.º 4, do Regulamento (UE) 2016/679.

([10]) Em maio de 2021, o *England and Wales Court of Appeal* (Tribunal de Recurso da Inglaterra e do País de Gales) tinha considerado incompatível com a legislação do Reino Unido a isenção relativa à imigração conforme formulada na altura no ponto 4 (1) do *schedule* 2 da *Data Protection Act* do Reino Unido, uma vez que a medida legislativa não continha disposições específicas que estabelecessem as garantias enumeradas no artigo 23.º, n.º 2, do RGPD do Reino Unido. A fim de dar cumprimento ao acórdão, o Governo do Reino Unido reviu a isenção relativa à imigração, aprovando os *Data Protection Act 2018 (Amendment of Schedule 2 Exemptions) Regulations 2022* [Regulamentos de 2022 que alteram o *Schedule* 2 (Isenções) da Lei relativa à Proteção de Dados]. No entanto, a isenção revista foi novamente impugnada com base no facto de não cumprir todos os requisitos do artigo 23.º, n.º 2, do RGPD do Reino Unido. Num acórdão de 11 de dezembro de 2023, o *Court of Appeal* (Tribunal de Recurso) declarou novamente a isenção relativa à imigração revista incompatível com o artigo 23.º, n.º 2, do RGPD do Reino Unido. Para dar cumprimento, o Governo do Reino Unido aprovou então os *Data Protection Act 2018 (Amendment of Schedule 2 Exemptions) Regulations 2024* [Regulamentos de 2024 que alteram o *Schedule* 2 (Isenções) da Lei relativa à Proteção de Dados], que entraram em vigor em 8 de março de 2024.

2. DESENVOLVIMENTOS PERTINENTES RELATIVOS ÀS NORMAS APLICÁVEIS AO TRATAMENTO DE DADOS PESSOAIS

2.1. Quadro do Reino Unido relativo à proteção de dados

(9) Quando a Decisão de Execução (UE) 2021/1772 foi adotada, o quadro da proteção dos dados pessoais no Reino Unido era composto pelos seguintes diplomas:

— o RGPD do Reino Unido ([11]), conforme incorporado no direito do Reino Unido ao abrigo da *European Union (Withdrawal) Act 2018* [Lei de 2018 sobre (a Saída da) União Europeia] ([12]) e alterado pelos *Data Protection, Privacy and Electronic Communications (Amendments etc.) EU Exit) Regulations 2019 (DPPEC Regulations)* [Regulamentos de 2019 relativos à Proteção de Dados, à Privacidade e às Comunicações Eletrónicas (alterações, etc.) (Saída da UE) — Regulamentos DPPEC] ([13]),

— a DPA 2018 ([14]), com a redação que lhe foi dada pelos Regulamentos DPPEC.

(10) Embora estas duas leis, que refletiram de perto as regras correspondentes aplicáveis na União Europeia, continuem a constituir a legislação do Reino Unido relativa à proteção de dados, as mesmas têm sido, desde então, objeto de alterações limitadas, refletindo que o Reino Unido deixou de estar sujeito ao direito da União Europeia.

(11) Em primeiro lugar, a *Retained EU Law (Revocation and Reform) Act 2023* [Lei de 2023 relativa ao Direito da UE Mantido (Revogação e Reforma) — Lei REUL] ([15]) esclareceu que os princípios gerais do direito da UE já não faziam parte do direito interno do Reino Unido após o final de 2023 ([16]). Além disso, os órgãos jurisdicionais do Reino Unido já não têm a obrigação de interpretar «direito equiparado» não alterado, anteriormente designado por «direito da UE mantido», em conformidade com os princípios gerais do direito da UE, devendo esse direito ser interpretado, ao invés, de forma compatível com o direito interno do Reino Unido ([17]). No entanto, o direito equiparado não alterado tem de continuar a ser interpretado pelos órgãos jurisdicionais competentes do Reino Unido em conformidade com a jurisprudência pertinente do Tribunal de Justiça da União Europeia proferida antes do fim do período de transição ([18]), como também mencionado no considerando 13 da Decisão de Execução (UE) 2021/1772. A DPA 2018 foi alterada pela *Data (Use and Access) Act* para clarificar o efeito da Lei REUL na legislação do Reino Unido relativa à proteção de dados. Por exemplo, a *section 183A*(1) da DPA 2018 prevê, como regra geral, que qualquer legislação nova (aprovada a partir de 20 de agosto de 2025) que introduza novas obrigações ou poderes para o tratamento de dados pessoais se presuma sujeita à legislação do Reino Unido relativa à proteção de dados. Isto significa que o quadro de proteção de dados do Reino Unido continua a prevalecer em

([11]) *General Data Protection Regulation* [não traduzido para português], disponível na seguinte ligação: https://www.legislation.gov.uk/eur/2016/679/contents.

([12]) A *European Union (Withdrawal) Act 2018* [não traduzida para português], disponível na seguinte ligação: https://www.legislation.gov.uk/ukpga/2018/16/contents, incorporou legislação da União que era diretamente aplicável no Reino Unido até ao fim do período de transição na legislação do Reino Unido. O denominado «direito da UE mantido» incluía o Regulamento (UE) 2016/679 na sua totalidade, incluindo os seus considerandos [ver as Notas Explicativas da *European Union (Withdrawal) Act 2018*, n.º 83, disponíveis na seguinte ligação: https://www.legislation.gov.uk/ukpga/2018/16/pdfs/ukpgaen_20180016_en.pdf]. Em conformidade com essa lei, o direito da UE mantido que não foi alterado devia ser interpretado pelos órgãos jurisdicionais do Reino Unido à luz da jurisprudência pertinente do Tribunal de Justiça da União Europeia e dos princípios gerais do direito da União, uma vez que produziram efeitos imediatamente antes do termo do período de transição (respetivamente, «jurisprudência da UE mantida» e «princípios gerais do direito da UE mantidos»).

([13]) Os *Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019*, disponíveis na seguinte ligação: https://www.legislation.gov.uk/uksi/2019/419/contents/made, com a redação que lhe foi dada pelos Regulamentos DPPEC 2020, disponíveis na seguinte ligação: https://www.legislation.gov.uk/ukdsi/2020/9780348213522. Os Regulamentos DPPEC alteram o Regulamento (UE) 2016/679 conforme incorporado na legislação do Reino Unido através da *European Union (Withdrawal) Act 2018* [Lei de 2018 sobre (a Saída da) União Europeia], da DPA 2018 e de outra legislação relativa a proteção de dados de forma que se enquadre no contexto nacional.

([14]) *Data Protection Act 2018*, disponível na seguinte ligação: https://www.legislation.gov.uk/ukpga/2018/12/contents. Antes da saída do Reino Unido da União Europeia e durante o período de transição, a DPA 2018 estabeleceu regras nacionais, quando permitido pelo Regulamento (UE) 2016/679, especificando e limitando a aplicação das regras do Regulamento (UE) 2016/679, e transpôs a 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 (JO L 119 de 4.5.2016, p. 89, ELI: http://data.europa.eu/eli/dir/2016/680/oj).

([15]) Disponível na seguinte ligação: https://www.legislation.gov.uk/ukpga/2023/28.

([16]) *Section* 5 da *European Union (Withdrawal) Act 2018*, com a redação que lhe foi dada pela Lei REUL.

([17]) *Section* 5(A2) da *European Union (Withdrawal) Act 2018*, com a redação que lhe foi dada pela Lei REUL.

([18]) *Section* 6(3) e (7) da *European Union Withdrawal Act 2018*, com a redação que lhe foi dada pela Lei REUL.

relação a qualquer outra legislação. Nos termos da *section* 183A(2)(b) da DPA 2018, esta presunção pode não aplicar-se se o Parlamento do Reino Unido decidir deliberadamente nesse sentido de forma expressa na legislação, preservando a soberania parlamentar. Além disso, a *section* 186(2A) da DPA 2018 clarifica que as restrições aos direitos dos titulares dos dados, enumeradas na *section* 186(3) da DPA 2018, não são derrogadas pela *section* 186(1) da DPA 2018, a qual prevê que os atos que proíbam ou restrinjam a divulgação de informações não precludem determinados direitos de proteção de dados. Desta forma, garante-se que, por exemplo, as restrições aos direitos dos titulares dos dados, previstas na DPA 2018, não são abrangidas pela «derrogação à proteção de dados» geral prevista na *section* 186(1) da DPA 2018.

(12) Em segundo lugar, desde a adoção da Decisão de Execução (UE) 2021/1772, a legislação do Reino Unido relativa à proteção de dados foi alterada pelos *Data Protection (Fundamental Rights and Freedoms) Amendment Regulations 2023* [Regulamentos de Alteração de 2023 relativos à Proteção de Dados (Direitos e Liberdades Fundamentais)] ([19]). Estes regulamentos definem as referências aos direitos fundamentais ou às liberdades fundamentais no RGPD do Reino Unido e na DPA 2018 [anteriormente definidas como abrangendo os direitos fundamentais e as liberdades fundamentais da UE ([20])], como referências aos direitos ao abrigo da Convenção Europeia dos Direitos Humanos, direitos que passaram a estar previstos na legislação nacional do Reino Unido no quadro da *Human Rights Act 1998* [Lei de 1998 relativa aos Direitos Humanos] ([21]). A *Human Rights Act 1998* incorpora os direitos constantes da Convenção Europeia dos Direitos Humanos no direito do Reino Unido. A *Human Rights Act* concede a todas as pessoas os direitos e as liberdades fundamentais previstos nos artigos 2.º a 12.° e no artigo 14.º da Convenção Europeia dos Direitos Humanos, nos artigos 1.º, 2.° e 3.° do seu Protocolo n.º 1, e no artigo 1.º do seu Protocolo n.º 13, em conjugação com os artigos 16.º, 17.° e 18.° da referida convenção. Tal inclui o direito ao respeito pela vida privada e familiar (e a proteção dos dados pessoais no âmbito desse direito), bem como o direito a um processo equitativo ([22]).

(13) Por último, o RGPD e a DPA 2018 foram objeto de reformas específicas previstas nas partes cinco e seis da *Data (Use and Access) Act*. Embora o âmbito de aplicação da *Data (Use and Access) Act* vá muito além da proteção dos dados pessoais, a mesma prevê alterações limitadas a vários aspetos do regime de proteção de dados, como, nomeadamente, as regras relativas ao tratamento dos dados para efeitos de investigação científica, as bases jurídicas para o tratamento de dados, as regras relativas ao princípio da limitação das finalidades e as condições para a tomada de decisões automatizadas. Além disso, a *Data (Use and Access) Act* introduz alterações à estrutura de governação do ICO. Uma vez implementadas, estas medidas conduzirão à substituição do ICO por uma nova entidade, a Comissão para a Informação. O papel e as funções da entidade reguladora enquanto autoridade independente de supervisão da proteção de dados no Reino Unido não irão sofrer alterações. Esta lei também introduz novos poderes de controlo do cumprimento para a entidade reguladora.

(14) A presente decisão avalia os desenvolvimentos no domínio legislativo, no domínio regulamentar, bem como noutros domínios, que sejam pertinentes para a conclusão relativa ao nível de proteção garantido pelo Reino Unido a que se chegou na Decisão de Execução (UE) 2021/1772. A avaliação feita na Decisão de Execução (UE) 2021/1772 continua a ser válida relativamente aos aspetos do quadro de proteção de dados do Reino Unido que não foi alterado ou afetado por outros desenvolvimentos desde a adoção da Decisão de Execução (UE) 2021/1772.

(15) Os desenvolvimentos pertinentes no domínio legislativo, no domínio regulamentar, bem como noutros domínios, são analisados pormenorizadamente nas secções seguintes com base no padrão de adequação, segundo o qual a Comissão tem de apurar se o país terceiro em causa assegura um nível de proteção «essencialmente equivalente» ao assegurado na União Europeia ([23]). Conforme esclareceu o Tribunal de Justiça da União Europeia, isto não significa que se exija um nível de proteção idêntico ([24]). Mais concretamente, os meios a que o país terceiro em causa recorre para proteger os dados pessoais podem ser diferentes dos implementados na União Europeia, desde que se revelem, na prática, efetivos para assegurar um nível adequado de proteção ([25]). Por conseguinte, o padrão de adequação não exige que as regras da União sejam replicadas ponto por ponto. Em vez disso, importa aferir sobretudo se, através do teor dos direitos em matéria de proteção de dados e da sua aplicação, controlo e execução efetivos, o ordenamento jurídico estrangeiro consegue, no seu conjunto, garantir o nível de proteção exigido ([26]).

([19]) Disponível na seguinte ligação: https://www.gov.uk/government/publications/the-data-protection-fundamental-rights-and-freedoms-amendment-regulations-2023.

([20]) Os direitos fundamentais e as liberdades fundamentais da UE foram mantidos no direito do Reino Unido na *Section* 4 da *European Union (Withdrawal) Act 2018*, a qual foi revogada no final de 2023 pela Lei REUL.

([21]) *Section* 2(3) of the *Data Protection (Fundamental Rights and Freedoms) Amendment Regulations 2023*.

([22]) Artigos 6.º, 8.°, 10.° e 13.° da CEDH (ver também o *schedule* 1 da *Human Rights Act 1998*).

([23]) Considerando 104 do Regulamento (UE) 2016/679.

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

([25]) Acórdão Schrems I, n.º 74.

([26]) Ver Comunicação da Comissão ao Parlamento Europeu e ao Conselho, Intercâmbio e proteção de dados pessoais num mundo globalizado, COM(2017) 7, de 10.1.2017, secção 3.1, p. 6, disponível na seguinte ligação: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52017DC0007&from=PT.

2.1.1. *Definições*

(16) Os conceitos básicos de proteção de dados que refletem a terminologia do Regulamento (UE) 2016/679 continuam a ser aplicados no regime de proteção de dados do Reino Unido. Estes conceitos foram avaliados no considerando 23 da Decisão de Execução (UE) 2021/1772.

(17) Embora a *Data (Use and Access) Act* deixe inalterada a grande maioria das definições, a mesma introduziu definições específicas relacionadas com o tratamento de dados pessoais para fins científicos, históricos e estatísticos no artigo 4.º, n.ºs 2, 3, 4 e 5, do RGPD do Reino Unido. O n.º 2 define «tratamento para fins científicos» como o tratamento de dados pessoais realizado para fins de investigação que possa razoavelmente ser descrita como científica. Esta investigação pode ser financiada por fundos públicos ou privados e ser realizada no âmbito de uma atividade comercial ou não comercial. Refletindo o conteúdo do considerando 159 do Regulamento (UE) 2016/679, o n.º 3 apresenta uma lista não exaustiva de exemplos de atividades de investigação consideradas para fins científicos, incluindo o desenvolvimento tecnológico, a demonstração, a investigação fundamental e a investigação aplicada. O n.º 4 esclarece que a «investigação histórica» inclui a investigação genealógica, que também é reconhecida como um objetivo histórico no considerando 160 do Regulamento (UE) 2016/679. Por último, o n.º 5 define tratamento para fins estatísticos como o tratamento de dados para inquéritos estatísticos ou para produzir resultados estatísticos, sempre que os dados sejam agregados quando deixem de constituir dados pessoais. Além disso, os dados tratados ou as informações resultantes não devem ser utilizados para tomar decisões ou tomar medidas dirigidas a qualquer pessoa. Esta definição está em consonância com a compreensão dos fins estatísticos, descrita no considerando 162 do Regulamento (UE) 2016/679.

(18) Em conclusão, embora as alterações ao artigo 4.º do RGPD do Reino Unido acrescentem definições específicas de tratamento de dados para fins científicos, históricos e estatísticos, essas definições são coerentes com a letra e o espírito do Regulamento (UE) 2016/679, como refletido nos considerandos 159, 160 e 162 acima referidos.

(19) Ao aditar o n.º 6 ao artigo 4.º do RGPD do Reino Unido, a *Data (Use and Access) Act* também estabeleceu um quadro específico para a obtenção do consentimento do titular dos dados para o tratamento de dados pessoais para fins científicos. Em termos muito semelhantes aos do considerando 33 do Regulamento (UE) 2016/679, que reconhece que, no domínio da investigação científica, nem sempre é possível obter consentimento para uma finalidade específica de tratamento, a nova disposição possibilita formas mais amplas de consentimento, permitindo que os titulares dos dados possam dar um consentimento válido mesmo quando as finalidades exatas da investigação não possam ser plenamente identificadas no momento da recolha dos dados, desde que o pedido de consentimento seja coerente com normas éticas geralmente reconhecidas pertinentes para o domínio de investigação específico. Em qualquer caso, os titulares dos dados devem ter a oportunidade de consentir no tratamento de dados pessoais apenas para partes específicas da investigação, sempre que possível.

(20) Por último, a *Data (Use and Access) Act* descreveu mais pormenorizadamente as garantias anteriormente estabelecidas no artigo 89.º do RGPD do Reino Unido e na *section* 19 da DPA 2018 para o tratamento de dados para fins de arquivo de interesse público e para fins de investigação científica, histórica e estatística num novo capítulo 8A do RGPD do Reino Unido ([27]). Estas garantias são semelhantes às exigidas pelo artigo 89.º do Regulamento (UE) 2016/679 e incluem a obrigação de prever medidas técnicas e organizativas para assegurar o respeito do princípio da minimização dos dados.

2.2. **Garantias, direitos e obrigações**

2.2.1. *Licitude e lealdade do tratamento*

(21) O quadro de proteção de dados do Reino Unido continua a prever que os dados devem ser objeto de um tratamento lícito, leal e legítimo, como avaliado nos considerandos 24 a 26 da Decisão de Execução (UE) 2021/1772.

([27]) Artigos 84A a 84D do RGPD do Reino Unido, na redação que lhe foi dada pela *section* 86 da *Data (Use and Access) Act*.

(22) Os princípios da licitude e lealdade, bem como os fundamentos para o tratamento lícito continuam a estar garantidos no direito do Reino Unido através do artigo 5(1)(a), e do artigo 6(1) do RGPD do Reino Unido, que estão avaliados na Decisão de Execução (UE) 2021/1772. Embora essas disposições permaneçam, em grande medida, idênticas ([28]) às correspondentes disposições do Regulamento (UE) 2016/679, a *Data (Use and Access) Act* altera, em primeiro lugar, o artigo 6(1) do RGPD do Reino Unido, ao introduzir um fundamento legal adicional para o tratamento de dados pessoais em conformidade com o artigo 6(1)(ea) ([29]). De acordo com essa disposição, o tratamento é lícito se e na medida em que for «necessário para efeitos de um interesse legítimo reconhecido». Ao contrário do fundamento jurídico do interesse legítimo constante do artigo 6(1)(f) do RGPD do Reino Unido, o novo fundamento jurídico de interesse legítimo reconhecido não exige uma ponderação caso a caso dos interesses legítimos do responsável pelo tratamento em relação com os interesses ou os direitos e liberdades fundamentais do titular dos dados, tendo por objetivo proporcionar uma maior segurança jurídica aos responsáveis pelo tratamento que não sejam organismos públicos. O artigo 6(5) do RGPD do Reino Unido, recentemente introduzido, especifica que o tratamento só é necessário para efeitos de um interesse legítimo reconhecido se preencher uma condição do anexo 1 ([30]), o qual enumera as situações em que o tratamento é considerado necessário para efeitos de um interesse legítimo reconhecido, por exemplo, quando ocorrer em resposta a um pedido recebido por uma autoridade pública que necessita dos dados para efeitos do exercício de uma missão de interesse público cuja base jurídica esteja em conformidade com o artigo 6(3) do RGPD do Reino Unido, sempre que o tratamento seja necessário para salvaguardar a segurança nacional, proteger a segurança pública ou para fins de defesa, responder a uma emergência, detetar, investigar ou prevenir a criminalidade ou proteger pessoas vulneráveis ([31]).

(23) Embora a *Data (Use and Access) Act* alargue, assim, a lista de fundamentos jurídicos para o tratamento de dados pessoais de que o responsável pelo tratamento dispõe, o novo fundamento jurídico de interesse legítimo reconhecido está sujeito a várias limitações importantes. Em primeiro lugar, os interesses legítimos reconhecidos limitam-se a situações específicas, taxativamente enumeradas na lei. Em segundo lugar, este fundamento jurídico não pode ser invocado pelas autoridades públicas no exercício das suas funções ([32]). Em terceiro lugar, apenas diz respeito a domínios em que existe um interesse público manifesto na atividade de tratamento (de acordo com as condições previstas no anexo 1), ou seja, em que o tratamento serve os objetivos enumerados no artigo 23.º do RGPD do Reino Unido [que corresponde ao artigo 23.º do Regulamento (UE) 2016/679] e, por conseguinte, não pode ser invocado para fins comerciais. Em quarto lugar, embora a *Data (Use and Access) Act* conceda ao ministro

([28]) Para efeitos de clarificação, a *Data (Use and Access) Act* também introduz no artigo 6.º do RGPD do Reino Unido um novo número que fornece exemplos de tipos de tratamento que podem ser considerados necessários para efeitos de interesse legítimo na aceção do artigo 6.º, n.º 1, alínea f), do RGPD do Reino Unido. Esses exemplos (comercialização direta, transmissão intragrupo de dados para fins administrativos e segurança das redes e dos sistemas de informação) também são mencionados nos considerandos 47 e 48 do Regulamento (UE) 2016/679 como situações em que o tratamento seria considerado no interesse legítimo do responsável pelo tratamento.

([29]) *Section* 70(2)(b) da *Data (Use and Access) Act*. A *section* 70(5) da *Data (Use and Access) Act* alargou o direito de oposição previsto no artigo 21.º do RGPD do Reino Unido ao novo artigo 6(1)(ea), do RGPD do Reino Unido.

([30]) *Section* 70(4) da *Data (Use and Access) Act*.

([31]) Ver *schedule* 4 da *Data (Use and Access) Act*. De acordo com as autoridades do Reino Unido, os exemplos de situações em que organismos não públicos podem ter de tratar dados pessoais para prevenir ou detetar a criminalidade incluem uma empresa que toma conhecimento de tentativas de piratear ilegalmente os seus sistemas informáticos, ou um banco ou instituição financeira que toma conhecimento de tentativas fraudulentas de abrir uma conta. O tratamento de dados pessoais por um organismo não público pode ser necessário, por exemplo, para salvaguardar a segurança ou a defesa nacionais se uma organização comercial suspeitar que a atividade em linha de um cliente indicou o envolvimento numa atividade terrorista. O ICO está a elaborar orientações específicas a este respeito, incluindo uma definição dos conceitos relevantes. Por exemplo, refere-se ao facto de a expressão «segurança nacional» ser suscetível de abranger a segurança e o bem-estar do Reino Unido no seu conjunto, da sua população, das suas instituições e do seu sistema de governo. Queira consultar o projeto de orientações do ICO sobre o interesse legítimo reconhecido, conforme publicado para consulta pública, disponível na seguinte ligação: https://ico.org.uk/for-organisations/recognised-legitimate-interest-guidance/.

([32]) Artigo 6(1), na redação que lhe foi dada pela *section* 70(2)(c) da *Data (Use and Access) Act*.

da tutela o direito de alterar a lista do anexo 1 por meio de regulamento ([33]), o ministro da tutela só pode adotar esse regulamento após consultar o ICO ([34]) e acrescentar um interesse legítimo reconhecido a essa lista se esse tratamento for novamente necessário para salvaguardar um objetivo de interesse público enumerado no artigo 23(1)(c) a (j) do RGPD do Reino Unido ([35]). Por último, conforme igualmente confirmado pelas orientações do ICO ([36]), os responsáveis pelo tratamento que invoquem como base jurídica um interesse legítimo reconhecido são obrigados a cumprir todos os outros requisitos previstos no RGPD do Reino Unido, nomeadamente garantir que o tratamento é necessário e proporcionado para alcançar o interesse legítimo.

(24) Em segundo lugar, a *Data (Use and Access) Act* esclarece, nos artigos 6.º, n.º 3, 9.°, n.º 2, alínea g), e 10.°, n.º 1, do RGPD do Reino Unido, que correspondem às respetivas disposições do Regulamento (UE) 2016/679, que o fundamento para o tratamento de dados pessoais, categorias especiais de dados pessoais e dados pessoais relacionados com condenações penais e infrações para o cumprimento de uma obrigação legal ou no exercício de funções de interesse público pode ter uma base não só no direito nacional, mas também no direito internacional aplicável ([37]). O direito internacional aplicável é então limitado pelo novo artigo 9.º-A do RGPD do Reino Unido, em conjugação com o *schedule A1*, a um único acordo, a saber, o *Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime* [Acordo entre o Governo do Reino Unido da Grã-Bretanha e da Irlanda do Norte e o Governo dos Estados Unidos da América relativo ao Acesso aos Dados Eletrónicos para Efeitos de Combate à Criminalidade Grave], assinado em 3 de outubro de 2019 (Acordo Reino Unido-EUA) ([38]). As garantias previstas nesse acordo foram avaliadas nos considerandos 153 a 155 da Decisão de Execução (UE) 2021/1772 e a sua aplicação é avaliada nos considerandos 87 a 93 da presente decisão.

2.2.2. *Tratamento de categorias especiais de dados pessoais*

(25) O quadro de proteção de dados do Reino Unido continua a prever garantias específicas quando estão envolvidas categorias especiais de dados, como avaliado nos considerandos 27 a 42 da Decisão de Execução (UE) 2021/1772.

(26) Tanto a definição de categorias especiais de dados pessoais como as regras específicas aplicáveis ao tratamento destas categorias de dados constantes do RGPD do Reino Unido e da DPA 2018 permanecem em vigor. Simultaneamente, a *Data (Use and Access) Act* confere ao ministro da tutela novos poderes legislativos para acrescentar categorias especiais de dados, adaptar as condições aplicáveis à sua utilização e acrescentar novas definições, se necessário ([39]). É importante salientar que a *Data (Use and Access) Act* não permite que o ministro da tutela suprima ou altere categorias especiais de dados existentes nem alterar as condições para o tratamento dessas categorias ([40]). Por conseguinte, o novo poder regulamentar permite apenas ao Governo acrescentar novas categorias de dados sensíveis e determinar as condições para o tratamento dessas categorias, o que se destina a permitir que o Governo responda a futuros desenvolvimentos tecnológicos e societais quando necessário.

(27) Por conseguinte, estas alterações não afetam o nível de proteção das categorias especiais de dados pessoais consideradas essencialmente equivalentes à proteção na UE na Decisão de Execução (UE) 2021/1772.

([33]) Antes de adotar regulamentos, o ministro da tutela deve ter em conta os efeitos de quaisquer alterações nos interesses e nos direitos e liberdades fundamentais dos titulares dos dados, bem como o facto de as crianças (se for caso disso) merecerem proteção específica no que diz respeito aos seus dados pessoais. Os regulamentos devem ser adotados por instrumento estatutário e estão sujeitos ao procedimento de resolução positiva, o que significa que devem ser expressamente aprovados pelo Parlamento do Reino Unido. *Section* 70(4)(8) da *Data (Use and Access) Act*.

([34]) *Section* 182(2) da DPA 2018.

([35]) *Section* 70(4)(9) da *Data (Use and Access) Act*.

([36]) Queira consultar as orientações do ICO sobre interesses legítimos na seguinte ligação: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/legitimate-interests/?q=appropriate+policy.

([37]) *Section* 72 da *Data (Use and Access) Act*.

([38]) Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America on Access to Electronic Data for the Purpose of *Countering Serious Crime*, disponível na seguinte ligação: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/836969/CS_USA_6.2019_Agreement_between_the_United_Kingdom_and_the_USA_on_Access_to_Electronic_Data_for_the_Purpose_of_Countering_Serious_Crime.pdf.

([39]) *Section* 74 da *Data (Use and Access) Act*. Esses diplomas estão sujeitos ao procedimento de resolução positiva, o que significa que exigem a aprovação expressa do Parlamento do Reino Unido.

([40]) Ver novo artigo 11A(1)(b) e (2) do RGPD do Reino Unido, bem como as Notas Explicativas do *Data (Use and Access) Bill*, n.º 571, disponível na seguinte ligação: https://publications.parliament.uk/pa/bills/cbill/59-01/0179/en/240179en.pdf.

2.2.3. *Limitação das finalidades*

(28) O regime de proteção de dados pessoais do Reino Unido continua a prever que os dados devem ser tratados com uma finalidade específica e, subsequentemente, utilizados apenas na medida em que essa utilização não seja incompatível com a finalidade do tratamento, como avaliado nos considerandos 43 a 48 da Decisão de Execução (UE) 2021/1772.

(29) Em primeiro lugar, a *Data (Use and Access) Act* introduz algumas alterações específicas ao princípio da limitação das finalidades previsto no artigo 5(1)(b) do RGPD do Reino Unido. Estas alterações clarificam a aplicação deste princípio sem alterar a essência. A *section* 71(1), (2) e (3) da *Data (Use and Access) Act* especifica que o princípio da limitação das finalidades se aplica quando os dados são recolhidos junto do titular dos dados ou de outra forma, que só é aplicável quando os dados pessoais são posteriormente tratados pelo mesmo responsável pelo tratamento ou em seu nome (ou seja, que não se aplica em caso de mudança de responsável pelo tratamento) e que o tratamento não é lícito pelo simples facto de ser compatível com as finalidades para as quais os dados pessoais foram recolhidos.

(30) Em segundo lugar, a *Data (Use and Access) Act* clarifica as regras relativas ao tratamento posterior de dados pessoais, agrupando-as no novo artigo 8A do RGPD do Reino Unido, que estabelece o regime integral para o tratamento posterior de dados pessoais. O artigo 8A(2) do RGPD do Reino Unido enumera os elementos a ter em conta para determinar se uma nova finalidade de tratamento é compatível com a finalidade inicial. Estes elementos estavam anteriormente enumerados no artigo 6.º, n.º 4, do RGPD do Reino Unido, que corresponde ao artigo 6.º, n.º 4, do Regulamento (UE) 2016/679 ([41]). O artigo 8A(3) do RGPD do Reino Unido agrupa numa única disposição as situações em que o tratamento de dados pessoais para uma nova finalidade deve ser considerado compatível com a finalidade inicial. Abrange as situações em que o titular dos dados consente no tratamento de dados pessoais para a nova finalidade ou em que o tratamento seja necessário para salvaguardar um dos objetivos enumerados no artigo 23.º, n.º 1 ([42]), quando o tratamento for efetuado para fins de investigação científica ou histórica, de arquivo de interesse público ou para fins estatísticos ([43]). Por último, a *Data (Use and Access) Act* esclarece que qualquer tratamento efetuado para assegurar que o tratamento cumpre os princípios de proteção de dados estabelecidos no artigo 5(1) do RGPD do Reino Unido ou que demonstre que o faz é considerado compatível com a finalidade inicial. As situações acima referidas continuam a corresponder ao tratamento posterior considerado compatível também no Regulamento (UE) 2016/679.

(31) Em terceiro lugar, a *Data (Use and Access) Act* também introduz no artigo 8A(3)(d) do RGPD do Reino Unido novas situações em que se considera que o tratamento de dados pessoais para uma nova finalidade é compatível com a finalidade inicial. Essas situações estão enumeradas no anexo 2 do RGPD do Reino Unido ([44]) e incluem, por exemplo, situações em que o tratamento é efetuado em resposta a um pedido recebido por uma autoridade pública que necessita dos dados para efeitos do exercício de uma missão de interesse público cuja base jurídica esteja em conformidade com o artigo 6.º, n.º 3, do RGPD do Reino Unido, em que o tratamento seja necessário para proteger a segurança pública, responder a uma emergência, detetar, investigar ou prevenir a criminalidade, proteger os interesses vitais do titular dos dados e outros, proteger pessoas vulneráveis, para efeitos fiscais ou, se necessário, para cumprir uma obrigação legalmente imposta ([45]).

(32) Embora a *Data (Use and Access) Act* acrescente, assim, situações à lista de situações em que se considera o tratamento posterior para uma finalidade diferente compatível com a finalidade inicial do tratamento, esse acréscimo está sujeito a limitações importantes. Em primeiro lugar, está limitado a situações específicas, taxativamente enumeradas na lei. Em segundo lugar, apenas diz respeito a domínios em que existe um interesse público manifesto na atividade de tratamento, ou seja, em que o tratamento posterior serve os objetivos enumerados no artigo 23.º do

([41]) À semelhança do Regulamento (UE) 2016/679, estes elementos incluem qualquer ligação entre a finalidade inicial e a nova finalidade, o contexto em que os dados pessoais foram recolhidos, incluindo a relação entre o titular dos dados e o responsável pelo tratamento, a natureza do tratamento e se este inclui categorias especiais de dados, as possíveis consequências do tratamento previsto para o titular dos dados e a existência de garantias adequadas.

([42]) Ver também o artigo 6.º, n.º 4, do Regulamento (UE) 2016/679.

([43]) Considerando 50 do Regulamento (UE) 2016/679.

([44]) O anexo 2 é introduzido no RGPD do Reino Unido através do *schedule* 5 da *Data (Use and Access) Act* — ver *section* 71(6) desta.

([45]) Ver *schedule* 5 da *Data (Use and Access) Act*.

RGPD do Reino Unido [que corresponde ao artigo 23.º do Regulamento (UE) 2016/679]. Por conseguinte, não pode ser invocado para fins comerciais. Em terceiro lugar, embora a *Data (Use and Access) Act* conceda ao ministro da tutela o direito de alterar a lista do anexo 2 por meio de regulamento ([46]), o ministro da tutela só pode acrescentar tipos de tratamento a essa lista se esse tratamento for novamente necessário para salvaguardar um objetivo de interesse público enumerado no artigo 23(1)(c) a (j), do RGPD do Reino Unido ([47]). Em quarto lugar, se a recolha de dados pessoais pelo responsável pelo tratamento se basear no consentimento do titular dos dados, o tratamento para uma nova finalidade nas situações enumeradas no anexo 2 só é considerado compatível com a finalidade inicial se não se puder razoavelmente esperar que o responsável pelo tratamento obtenha novo consentimento do titular dos dados ([48]).

2.2.4. *Direitos individuais*

(33) No quadro do Reino Unido, os titulares dos dados continuam a beneficiar, para a proteção dos dados pessoais, dos mesmos direitos individuais que os previstos no Regulamento (UE) 2016/679 sem alterações significativas ([49]), que podem ser exercidos perante o responsável pelo tratamento ou o subcontratante, especialmente o direito de acesso aos dados, o direito de oposição ao tratamento e o direito de retificação e apagamento dos dados, como avaliado nos considerandos 51 a 54 da Decisão de Execução (UE) 2021/1772.

(34) Em primeiro lugar, a *Data (Use and Access) Act* esclarece determinadas modalidades ao abrigo das quais esses direitos podem ser exercidos. Por um lado, especifica, através de uma alteração do artigo 12.º e da introdução de um novo artigo 12.º-A do RGPD do Reino Unido ([50]), os prazos dentro dos quais os responsáveis pelo tratamento têm de responder aos pedidos do titular dos dados. Mais especificamente, o artigo 12.º do RGPD do Reino Unido é alterado de modo a que o responsável pelo tratamento deixe de ser obrigado a prestar informações sobre as medidas tomadas (ou sobre os motivos para não ter tomado nenhuma medida) em resposta a um pedido do titular dos dados nos termos dos artigos 15.º a 22.° do RGPD do Reino Unido «no prazo de um mês a contar da receção do pedido», mas «antes do termo do prazo aplicável». O «prazo aplicável» é posteriormente definido no novo artigo 12.º-A do RGPD do Reino Unido como o período de um mês, com início na data pertinente, ou seja, quando o responsável pelo tratamento recebe o pedido, quando o responsável pelo tratamento recebe as informações solicitadas em relação a um pedido ao abrigo do artigo 12.º, n.º 6 do RGPD do Reino Unido, ou quando é paga a taxa cobrada em relação ao pedido ao abrigo do artigo 12.º, n.º 5 do RGPD do Reino Unido, consoante a data que for posterior ([51]). O artigo 12A(3) permite ainda ao responsável pelo tratamento prorrogar o prazo aplicável por mais dois meses, se tal for necessário devido à complexidade dos pedidos apresentados pelo titular dos dados ou ao número desses pedidos. Por outro lado, no que diz respeito apenas ao direito de acesso às informações e aos dados pessoais, a *Data (Use and Access) Act* altera o artigo 15.º do RGPD do Reino Unido a fim de incluir a clarificação desenvolvida no âmbito da jurisprudência nacional existente — com base no princípio da proporcionalidade consagrado no direito da UE — de que os responsáveis pelo tratamento apenas têm de efetuar pesquisas razoáveis e proporcionadas das informações e dos dados pessoais solicitados ([52]). Espera-se que a nova disposição seja interpretada em consonância com a jurisprudência existente, que estabelece que «[…] *a ponderação efetuada no exercício de proporcionalidade incide sobre a finalidade da pesquisa, nomeadamente os eventuais benefícios que a disponibilização das informações pode gerar para o titular dos dados, quando contrapostos com os meios utilizados para obter essas informações. Será necessário avaliar, caso a caso, se os esforços exigidos para obter e disponibilizar as informações são desproporcionados, quando comparados com os benefícios potencialmente gerados para o titular dos dados*» ([53]).

([46]) Artigo 8A(5) do RGPD do Reino Unido, na redação que lhe foi dada pela *section* 71(1) da *Data (Use and Access) Act*.
([47]) Artigo 8A(6) do RGPD do Reino Unido, na redação que lhe foi dada pela *section* 71(1) da *Data (Use and Access) Act*.
([48]) Artigo 8A(4)(b) do RGPD do Reino Unido, na redação que lhe foi dada pela *section* 71(1) da *Data (Use and Access) Act*.
([49]) A *section* 31 da *Victims and Prisoners Act 2024* [Lei de 2024 relativa às Vítimas e Prisioneiros (Lei VAP)] introduziu um fundamento adicional no direito ao apagamento previsto no artigo 17.º do RGPD do Reino Unido, concedendo aos titulares dos dados o direito de solicitar aos responsáveis pelo tratamento que apaguem os seus dados pessoais quando estes tenham sido tratados na sequência de uma alegação infundada sobre o titular dos dados apresentada por uma pessoa mal-intencionada. Uma pessoa é considerada «mal--intencionada» se tiver sido condenada por uma infração especificada na *section* 31(3) da Lei VAP (como, por exemplo, assédio) ou for objeto de uma decisão de proteção em casos de perseguição. A Lei VAP está disponível na seguinte ligação: https://www.legislation.gov.uk/ukpga/2024/21/contents. Além disso, a *section* 77 da *Data (Use and Access) Act* altera o direito à informação como previsto no artigo 13.º do RGPD do Reino Unido, de modo que o responsável pelo tratamento deixe de ser obrigado a informar o titular dos dados sobre o tratamento posterior dos seus dados pessoais para uma nova finalidade se essas finalidades forem de investigação científica ou histórica, de arquivo de interesse público ou de uma finalidade estatística, o tratamento for efetuado em conformidade com as garantias específicas estabelecidas no novo artigo 84B do RGPD do Reino Unido e se a prestação das informações for impossível ou desproporcionada.
([50]) *Section* 76 da *Data (Use and Access) Act*.
([51]) Artigo 12A(1) e (2) do RGPD do Reino Unido, na redação que lhe foi dada pela *section* 76 da *Data (Use and Access) Act*.
([52]) Artigo 15(1A) do RGPD do Reino Unido, na redação que lhe foi dada pela *section* 78 da *Data (Use and Access) Act*.
([53]) *Dawson-Dammer/Taylor Wessing LLP* [2017] EWCA Civ 74.

(35) Por conseguinte, embora os prazos de resposta aos pedidos dos titulares dos dados e as obrigações específicas dos responsáveis pelo tratamento relativamente ao direito de acesso estejam sujeitos a regras mais pormenorizadas, o sistema do Reino Unido continua a assegurar que os pedidos dos titulares dos dados têm de ser tratados em prazos razoáveis, definidos com base em fatores objetivos. Além disso, as obrigações substantivas do responsável pelo tratamento na resposta a pedidos de acesso são enquadradas com base em normas jurídicas estabelecidas que também têm em conta os interesses do titular dos dados. Por último, as atuais orientações do ICO já determinam que o responsável pelo tratamento não é obrigado a realizar pesquisas que sejam pouco razoáveis ou desproporcionadas face à importância de facultar o acesso às informações ([54]).

(36) As restrições a estes direitos individuais estabelecidas na DPA 2018 e que se enquadram no âmbito do artigo 23.º do RGPD do Reino Unido, bem como as limitações e garantias que enquadram a aplicação dessas restrições, continuam em vigor no quadro do Reino Unido ([55]), conforme descrito pormenorizadamente nos considerandos 55 a 67 da Decisão de Execução (UE) 2021/1772.

(37) No que diz especificamente respeito à restrição dos dados pessoais tratados para efeitos de manutenção de um controlo efetivo da imigração, ou à investigação ou deteção de atividades que prejudicariam a manutenção de um controlo efetivo da imigração, uma vez que a aplicação dessas disposições seria suscetível de prejudicar qualquer uma dessas questões (isenção relativa à imigração) ([56]), o Governo do Reino Unido alterou o n.º 4 do *schedule* 2 da DPA 2018 através dos *Data Protection Act 2018 (Amendment of Schedule 2 Exemptions) Regulations 2022* ([57]) e dos *Data Protection Act 2018 (Amendment of Schedule 2 Exemptions) Regulations 2024* [Regulamentos de 2024 que alteram o *Schedule* 2 (Isenções) da Lei relativa à Proteção de Dados] ([58]) que complementam os *Regulations 2022* ([59]). As alterações integram as garantias para o exercício da isenção relativa à imigração, exigidas pelo artigo 23.º, n.º 2, do RGPD do Reino Unido, nos n.ºs 4A e 4B do *schedule* 2 da DPA 2018. Exigem especialmente que i) a isenção relativa à imigração apenas seja invocada caso a caso, separadamente em relação a cada uma das disposições pertinentes do RGPD do Reino Unido e novamente em cada caso em que o ministro da tutela considere não aplicar ou restringir a aplicação de qualquer uma das disposições pertinentes do RGPD do Reino Unido ([60]), ii) os direitos e liberdades do titular dos dados e as possíveis vulnerabilidades sejam tidos em conta no exercício da isenção relativa à imigração ([61]), iii) o ministro da tutela mantenha um registo sobre a utilização da isenção relativa à imigração e informe o titular dos dados sobre a sua utilização (exceto em circunstâncias específicas em que as informações prejudiquem o objetivo da isenção) ([62]) e iv) esclareça que a utilização da isenção relativa à imigração está limitada ao tratamento de dados pessoais pelo ministro da tutela ([63]), ou seja, na prática, pelo Ministério da Administração Interna para as suas funções pertinentes para o *schedule* 2(4)(1) da DPA 2018. Além disso, explicam ainda o exercício de ponderação que deve ser realizado para determinar se o exercício dos direitos dos titulares dos dados é suscetível de prejudicar um controlo efetivo da imigração e se, consequentemente, é necessário e proporcionado restringir esses direitos.

([54]) Disponível na seguinte ligação: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/right-of-access/how-do-we-find-and-retrieve-the-relevant-information/.

([55]) A *section* 88(2) da *Data (Use and Access) Act* introduz uma pequena alteração à *section* 26(2)(f) da DPA 2018 (isenção relativa à segurança e defesa nacionais), esclarecendo que o direito de apresentar uma reclamação ao comissário em conformidade com o artigo 77.º do RGPD do Reino Unido não se inclui nas disposições cuja aplicação pode ser restringida para efeitos de segurança ou defesa nacionais.

([56]) Quando a Decisão de Execução (UE) 2021/1772 foi adotada, a validade e a interpretação da isenção relativa à imigração ao abrigo do direito do Reino Unido não tinham sido estabelecidas, na sequência de uma decisão do *England and Wales Court of Appeal* (Tribunal de Recurso da Inglaterra e do País de Gales), de 26 de maio de 2021, que considerou que a isenção relativa à imigração como constava da *DPA 2018* na altura, era incompatível com o direito do Reino Unido, uma vez que não continha disposições explícitas que estabelecessem as garantias enumeradas no artigo 23(2) do RGPD do Reino Unido que reflete o artigo 23.º, n.º 2, do Regulamento (UE) 2016/679. Por esse motivo, os dados pessoais transferidos para efeitos de controlo da imigração no Reino Unido, ou que de outra forma sejam abrangidos pelo âmbito de aplicação da isenção relativa à imigração, tinham sido excluídos do âmbito de aplicação da Decisão de Execução (UE) 2021/1772.

([57]) Os *Regulations* entraram em vigor em 31 de janeiro de 2022 e estão disponíveis na seguinte ligação: https://www.legislation.gov.uk/uksi/2022/76/contents/made.

([58]) Os *Regulations* entraram em vigor em 8 de março de 2024 e estão disponíveis na seguinte ligação: https://www.legislation.gov.uk/uksi/2024/342/contents/made.

([59]) A isenção relativa à imigração revista nas *Regulations 2022* foi novamente objeto de impugnação judicial com base no facto de não cumprir todos os requisitos do artigo 23(2) do RGPD do Reino Unido. Em dezembro de 2023, o *Court of Appeal* (Tribunal de Recurso) considerou essa isenção incompatível com os requisitos do artigo 23(2) do RGPD do Reino Unido. Na sequência desse acórdão, os *Regulations 2024* complementam os *Regulations 2022* e introduzem novas alterações à isenção relativa à imigração.

([60]) N.º 4A (2) do *schedule* 2 da DPA 2018.

([61]) N.º 4AB (3) e (4) do *schedule* 2 da DPA 2018. O Gabinete do Comissário para a Informação foi consultado sobre os projetos dos *Regulations 2024* e declarou publicamente que estava em conformidade com o regulamento. O ofício publicado em resposta à consulta e a confirmar a sua opinião está disponível na seguinte ligação: https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2024/02/ico-responds-to-home-office-s-draft-regulations-to-the-immigration-exemption/.

([62]) N.º 4B(1) e (2) do *schedule* 2 da DPA 2018.

([63]) N.º 4(1) do *schedule 2* da DPA 2018.

(38) Além disso, o ICO do Reino Unido emitiu orientações pormenorizadas sobre a utilização desta limitação específica ([64]). Essas orientações referem, especificamente, que «[n]ão se deve aplicar a isenção relativa à imigração como uma isenção geral para limitar […] os direitos para todos os dados detidos. O alcance da isenção está limitado aos direitos que, se exercidos relativamente aos dados detidos, prejudicariam as identificadas finalidades relativas à imigração. […]. Por conseguinte, a posição do responsável pelo tratamento deve ser, por norma, a de cumprir os requisitos do Regulamento (UE) 2016/679 e da DPA, na medida do possível. […] O teste do prejuízo tem um limiar elevado e a isenção não deve ser aplicada de forma genérica. […] Deve ponderar-se se a aplicação da isenção constitui uma resposta proporcionada ao pedido de proteção de dados da pessoa em causa. Caso se considere que existe uma necessidade social premente de aplicar a isenção relativa à imigração, deve também ser ponderado se essa necessidade se sobrepõe à obrigação para com as pessoas singulares ao abrigo do Regulamento (UE) 2016/679. Estas têm direitos relativamente aos seus dados pessoais que devem ser considerados em todas as circunstâncias, especialmente o direito de acesso. Por conseguinte, é importante que se considere, em todos os casos, se os direitos de proteção de dados da pessoa se sobrepõem ao risco identificado de prejuízo. A aplicação da isenção deve ser proporcionada às circunstâncias e é necessário que cada caso seja cuidadosamente considerado e documentado».

(39) De um modo geral, a restrição à imigração prevista no n.º 4 do *schedule* 2 da DPA 2018 como revista pelo Governo do Reino Unido em 2022 e 2024 e como interpretada pela jurisprudência ([65]) e pelas orientações do ICO, está sujeita a uma série de condições rigorosas que enquadram a sua aplicação e são muito semelhantes às condições estabelecidas no direito da União, nomeadamente no artigo 23.º do Regulamento (UE) 2016/679, em relação à restrição dos direitos e obrigações no domínio da proteção de dados para objetivos importantes de interesse público, como o controlo da imigração.

2.2.5. *Restrições relativas a transferências ulteriores*

(40) O nível de proteção conferido aos dados pessoais transferidos da União Europeia para responsáveis pelo tratamento ou subcontratantes no Reino Unido continua a não ser prejudicado pela transferência subsequente desses dados para destinatários num país terceiro. O regime relativo às transferências internacionais de dados pessoais do Reino Unido continua a ser muito semelhante ao das normas previstas no capítulo V do Regulamento (UE) 2016/679, conforme avaliado nos considerandos 74 a 82 da Decisão de Execução (UE) 2021/1772.

(41) Embora a *Data (Use and Access) Act* tenha alterado o capítulo 5 do RGPD do Reino Unido relativo às transferências de dados pessoais para países terceiros ou organizações internacionais, a mesma mantém o requisito fundamental de que os dados pessoais só podem ser transferidos para um país terceiro ou uma organização internacional quando a transferência se baseia em i) regulamentos que aprovam a transferência (nova terminologia para o que foi anteriormente referido como «regulamentos de adequação»), ii) garantias adequadas, ou iii) uma derrogação para situações específicas. Estes princípios gerais para as transferências de dados estão refletidos no novo artigo 44A que substitui o artigo 44.º do RGPD do Reino Unido ([66]), o qual também especifica que as transferências de dados pessoais para um país terceiro ou uma organização internacional só são permitidas se a transferência for efetuada em conformidade com as outras disposições do RGPD do Reino Unido.

(42) No que se refere especificamente aos regulamentos que aprovam uma transferência, o artigo 45A(2) do RGPD do Reino Unido especifica que o ministro da tutela só pode adotar esses regulamentos se considerar que o teste de proteção de dados se encontra satisfeito. Tal significa que a possibilidade introduzida no artigo 45A(3) do RGPD do Reino Unido de o ministro da tutela ter em conta a conveniência de facilitar os fluxos de dados ao adotar esses regulamentos encontra-se sempre sujeita à satisfação do teste de proteção de dados. A norma jurídica a cumprir relativamente ao teste de proteção de dados está prevista no novo artigo 45B(1) do RGPD do Reino Unido, que exige que o nível de proteção dos titulares dos dados nos países destinatários ou nas organizações internacionais não seja substancialmente inferior ao previsto para os titulares dos dados nos termos da legislação pertinente do Reino Unido relativa à proteção de dados. O artigo 45B(2) do RGPD do Reino Unido prevê uma lista não exaustiva de elementos a ter em conta ao avaliar se esse teste se encontra satisfeito, como o respeito pelo Estado de direito e pelos direitos humanos, a existência e os poderes de uma autoridade de proteção de dados, as modalidades de recurso judicial ou extrajudicial, as regras relativas à transferência de dados pessoais do país ou da organização para

([64]) Disponível na seguinte ligação: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/exemptions/immigration-exemption-a-guide/.

([65]) *Open Rights Group & Anor, R (On the Application Of)/Secretary of State for the Home Department & Anor* [2019] EWHC 2562 (Admin), n.os 40 e 41.

([66]) *Section* 85 e *schedule* 7 da *Data (Use and Access) Act*.

outros países ou organizações internacionais, as obrigações internacionais pertinentes do país ou organização e a constituição, tradições e cultura do país ou organização. Embora reformule a lista de elementos pertinentes prevista no anterior artigo 45.º do RGPD do Reino Unido, o novo artigo 45B(2) mantém os elementos essenciais dessa lista e, por conseguinte, mantém-se próximo do previsto no capítulo V do Regulamento (UE) 2016/679. Além disso, as autoridades do Reino Unido confirmaram que o ministro da tutela terá em conta elementos que não constam do artigo 45B(2), como as leis e práticas de um país terceiro relativas à forma como as autoridades públicas acedem aos dados pessoais para fins como a segurança nacional ou a aplicação da lei, na medida em que afetem o nível global de proteção. Além disso, as autoridades do Reino Unido consideram que a jurisprudência relevante no país terceiro constituirá uma componente essencial da análise das matérias enumeradas de forma não exaustiva no artigo 45B(2) do RGPD do Reino Unido.

(43) Os regulamentos que aprovam uma transferência continuam sujeitos aos requisitos processuais «gerais» previstos na *section* 182 da DPA 2018, conforme estabelecido no considerando 77 da Decisão de Execução (UE) 2021/1772. Ao abrigo deste procedimento, o ministro da tutela deve consultar o comissário para a informação ao propor a adoção dos regulamentos de adequação do Reino Unido. ([67]). Depois de adotados pelo ministro da tutela, esses regulamentos são apresentados ao parlamento e sujeitos ao procedimento de «resolução negativa», segundo o qual as câmaras do parlamento podem examinar os regulamentos e podem aprovar uma moção para anular os regulamentos no prazo de 40 dias ([68]).

(44) No que diz respeito às garantias adequadas, o novo artigo 46(1A) do RGPD do Reino Unido estabelece que essas transferências só podem ser efetuadas se os instrumentos disponíveis nos termos do artigo 46(2) e (3), ([69]) do RGPD do Reino Unido previrem garantias pertinentes e o responsável pelo tratamento, o subcontratante ou os organismos públicos em causa, agindo de forma razoável e proporcional, considerarem que o teste da proteção de dados está preenchido. Os novos n.os 6 e 7 esclarecem que o teste de proteção de dados está preenchido se, devido às garantias exigidas, o nível de proteção previsto para os titulares dos dados não for, após a transferência, substancialmente inferior ao nível previsto na legislação pertinente do Reino Unido relativa à proteção de dados, ou seja, como acontece ao abrigo do Regulamento (UE) 2016/679, as mesmas normas jurídicas aplicam-se aos dois regulamentos que aprovam uma transferência e garantias adequadas. Segundo o mesmo número, o razoável e proporcionado deve ser determinado em função de todas as circunstâncias, ou circunstâncias prováveis, da transferência ou do tipo de transferência, incluindo a natureza e o volume dos dados pessoais transferidos.

(45) No que diz respeito às derrogações para situações específicas, são introduzidas várias alterações técnicas no artigo 49.º do RGPD do Reino Unido, nas condições em que as derrogações a situações específicas podem ser aplicadas, que alinham a disposição com as alterações de outras disposições, mas não afetam o nível de proteção dos dados pessoais no Reino Unido. Além disso, é inserido um novo n.º 4A para reproduzir o efeito da *section* 18(1) da DPA 2018, que habilita o ministro da tutela a especificar, por via regulamentar, as circunstâncias das transferências de dados consideradas necessárias por razões de interesse público. Por último, um novo artigo 49A reproduz o efeito da *section* 18(2) da DPA 2018, que permite ao ministro da tutela, por via regulamentar, impor restrições às transferências de dados quando estas não forem aprovadas nos termos do artigo 45A (transferências aprovadas por regulamentos) e quando consideradas necessárias por razões importantes de interesse público.

(46) Em termos de aplicação das regras de transferência internacionais do Reino Unido, registaram-se vários desenvolvimentos desde a adoção da Decisão de Execução (UE) 2021/1772.

([67]) Ver o memorando de entendimento entre o ministro da tutela do Ministério dos Assuntos Digitais, da Cultura, dos Meios de Comunicação e do Desporto e o Gabinete do Comissário para a Informação sobre o papel do ICO em relação à nova avaliação da adequação do Reino Unido, disponível na seguinte ligação: https://www.gov.uk/government/publications/memorandum-of-understanding-mou-on-the-role-of-the-ico-in-relation-to-new-uk-adequacy-assessments.

([68]) Se esse voto for aprovado, em última instância, os regulamentos deixarão de ter efeito jurídico.

([69]) O instrumento de transferência disponível nos termos do artigo 46(2) e (3) do RGPD do Reino Unido é um instrumento juridicamente vinculativo e com força executiva entre autoridades ou organismos públicos, regras vinculativas para as empresas em conformidade com o artigo 47.º do RGPD do Reino Unido, cláusulas-tipo de proteção de dados especificadas em regulamentos adotados pelo ministro da tutela ou especificados num documento emitido pela Comissão para a Informação, um código de conduta aprovado e um mecanismo de certificação aprovado.

(47) No que diz respeito aos regulamentos que aprovam as transferências, foram adotados até à data dois novos regulamentos que refletem decisões de adequação que também estão em vigor na União, nomeadamente para as transferências para a República da Coreia e para as transferências para entidades comerciais que aderiram ao *United Kingdom Extension to the EU-U.S. Data Privacy Framework* [Extensão do Reino Unido ao Quadro relativo à Privacidade de Dados UE-EUA]. Os regulamentos de adequação para a República da Coreia ([70]) entraram em vigor em 19 de dezembro de 2022 e permitem a transferência de dados pessoais do Reino Unido para a República da Coreia. A *United Kingdom Extension to the EU-U.S. Data Privacy Framework*, em relação à qual a regulamentação pertinente ([71]) entrou em vigor em 12 de outubro de 2023, permite a livre circulação de dados pessoais para organizações certificadas dos EUA.

(48) No que diz respeito às garantias adequadas, o Reino Unido publicou as suas próprias cláusulas-tipo de proteção de dados, o *International Data Transfer Agreement* [Acordo relativo à Transferência Internacional de Dados] (IDTA) ([72]) e uma *Addendum to the EU Standard Contractual Clauses (SCCs)* [Adenda às cláusulas contratuais-tipo da UE (SCC)], diplomas que entraram em vigor em março de 2022. O IDTA prevê um mecanismo específico para o Reino Unido para assegurar garantias adequadas para a transferência de dados pessoais e partilha várias semelhanças com as SCC da UE. A adenda, emitida pelo ICO, permite que os responsáveis pelo tratamento de dados e os subcontratantes no Reino Unido recorram às SCC da UE ao abrigo do RGPD do Reino Unido para as transferências internacionais. O ICO também publicou o *Transfer Risk Assessment Tool* [Instrumento de Avaliação dos Riscos de Transferência] para apoiar as organizações do Reino Unido na avaliação dos riscos associados às transferências internacionais.

(49) O Reino Unido simplificou igualmente o processo de aprovação de regras vinculativas aplicáveis às empresas (BCR) através de novas orientações e de novas opções para as aprovar. Em julho de 2022, o ICO publicou orientações e quadros de referência para explicar a abordagem do Reino Unido em relação às BCR pós-Brexit e, em dezembro de 2023, foi publicada uma adenda às BCR da UE para assegurar que as BCR aprovadas ao abrigo do quadro da União têm força executiva no Reino Unido ([73]).

(50) Por último, em julho de 2023, o Reino Unido tornou-se membro associado do *Fórum Global Cross-Border Privacy Rules* (CBPR) ([74]). É importante salientar que esta qualidade de membro não implica qualquer facilitação das transferências de dados do Reino Unido para outros membros do Fórum CBPR. O Reino Unido esclareceu que qualquer transferência de dados pessoais do Reino Unido para países terceiros ou organizações internacionais tem de satisfazer as condições estabelecidas na legislação do Reino Unido, como acima descrito, especialmente o teste de proteção de dados, que exige que as normas de proteção concedidas não sejam «substancialmente inferiores» às previstas no RGPD do Reino Unido.

(51) Como a Comissão já explicou, os CBPR não asseguram um nível suficiente de proteção dos dados pessoais provenientes da UE. Concretamente, não confere direitos individuais oponíveis ([75]). Por conseguinte, é particularmente importante que, mesmo que o Reino Unido seja membro associado do Fórum Mundial CBPR, este último não possa constituir um mecanismo de transferência válido nos termos da legislação do Reino Unido relativa à proteção de dados. Se esta situação se alterasse, isso comprometeria o nível de proteção atualmente garantido aos dados pessoais transferidos da UE para o Reino Unido. Por conseguinte, a Comissão continuará a acompanhar de perto a evolução da situação neste domínio.

([70]) Disponível na seguinte ligação: https://www.legislation.gov.uk/uksi/2022/1213/made.

([71]) Disponível na seguinte ligação: https://www.legislation.gov.uk/uksi/2023/1028/made.

([72]) Disponível na seguinte ligação: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/international-transfers/international-data-transfer-agreement-and-guidance/

([73]) O ICO recebeu um número significativo de pedidos de aprovação de BCR do Reino Unido após o Brexit. Muitas BCR aprovadas já não podiam ser utilizadas, uma vez que só as BCR em que o ICO tinha estado envolvido no processo de aprovação podiam continuar a ser utilizadas após o Brexit, mas esses titulares de BCR eram obrigados a apresentar ao ICO documentação atualizada das BCR compatível com o RGPD.

([74]) O Fórum CBPR é composto pelos Estados Unidos da América, Canadá, Japão, República da Coreia, Filipinas, Singapura, Taiwan e Austrália; a Maurícia, o Centro Financeiro Internacional do Dubai e as Bermudas são membros associados como o Reino Unido.

([75]) Ver, por exemplo, a análise comparativa realizada pelas autoridades de proteção de dados do G7 sobre os principais elementos do regime de certificações do RGPD e do sistema CBPR, que revelou «diferenças assinaláveis» entre os sistemas, nomeadamente em matéria de «executoriedade e vias de recurso, regras relativas à supervisão independente e acesso governamental». Disponível na seguinte ligação: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/10063165
Ver considerando 79 da Decisão de Execução (UE) 2019/419 da Comissão, de 23 de janeiro de 2019, nos termos do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho sobre a adequação do nível de proteção dos dados pessoais assegurado pelo Japão no âmbito da Lei relativa à proteção de informações pessoais (JO L 76 de 19.3.2019, p. 1, ELI: http://data.europa.eu/eli/dec_impl/2019/419/oj).
Ver também Grupo de Trabalho do artigo 29.º, *Opinion 02/2014 on a referential for requirements for Binding Corporate Rules submitted to national Data Protection Authorities in the EU and Cross-Border Privacy Rules submitted to APEC CBPR Accountability Agents*, 6 de março de 2014.

2.2.6. *Decisões automatizadas*

(52) Embora mantendo vários elementos das regras relativas às decisões automatizadas avaliadas do considerando 54 da Decisão de Execução (UE) 2021/1772, a *Data (Use and Access) Act* alterou alguns aspetos dessas regras.

(53) Em primeiro lugar, o artigo 22B recentemente introduzido do RGPD do Reino Unido estabelece uma proibição geral do tratamento de categorias especiais de dados pessoais (definidos no artigo 9(1) do RGPD do Reino Unido) para decisões baseadas exclusivamente no tratamento automatizado que tenham efeitos jurídicos ou igualmente significativos para o titular dos dados. No entanto, esta proibição admite três exceções: se o titular dos dados tiver dado o seu consentimento explícito para esse tratamento; ou se a decisão for necessária para celebrar ou para executar um contrato entre o responsável pelo tratamento e o titular dos dados; ou se o tratamento for exigido ou autorizada por lei. Em relação às duas últimas exceções, o tratamento automatizado deve ser necessário por razões de interesse público importante ([76]). A proibição geral não se aplica às decisões significativas baseadas no tratamento automatizado de categorias não especiais de dados.

(54) Além disso, o novo artigo 22A do RGPD do Reino Unido esclarece a definição de decisão «baseada exclusivamente no tratamento automatizado», prevendo que é uma decisão em que não existe uma participação humana significativa no processo de tomada de decisão. É importante salientar que os responsáveis pelo tratamento são obrigados a avaliar em que medida a definição de perfis contribui para uma decisão de determinar se a participação humana tem sido significativa. O artigo 22A do RGPD do Reino Unido também esclarece que uma «decisão significativa» é uma decisão que produz efeitos jurídicos ou impactos igualmente significativos num titular dos dados ([77]).

(55) Em segundo lugar, o artigo 22C recentemente introduzido do RGPD do Reino Unido exige que os responsáveis pelo tratamento apliquem medidas para fornecer as garantias pertinentes para qualquer decisão significativa baseada total ou parcialmente em dados pessoais tomadas exclusivamente por tratamento automatizado (incluindo categorias não especiais de dados pessoais). Estas garantias devem incluir a prestação de informações ao titular dos dados sobre o processo de tomada de decisão, a possibilidade de o titular dos dados impugnar a decisão e apresentar observações e a garantia de que o titular dos dados pode obter uma intervenção humana no processo de tomada de decisão ([78]).

(56) Por último, o artigo 22D recentemente introduzido do RGPD do Reino Unido habilita o ministro da tutela a adotar legislação derivada para descrever o que constitui e o que não constitui uma participação humana significativa, e quais as decisões que devem ser consideradas e que não devem ser consideradas como tendo um efeito igualmente significativo para os titulares dos dados. Permite igualmente ao ministro da tutela adotar legislação derivada para i) acrescentar novas garantias; ii) impor requisitos que complementem as garantias existentes; e iii) definir medidas que não satisfaçam as garantias ([79]). Importa salientar que, antes de adotar regulamentos em conformidade com o artigo 22D do RGPD do Reino Unido, o ministro da tutela deve consultar o ICO ([80]), os regulamentos não podem alterar o artigo 22C do RGPD do Reino Unido ([81]) e estão sujeitos ao procedimento de resolução positiva ([82]), o que significa que têm de ser aprovados por ambas as câmaras do parlamento do Reino Unido antes de poderem ser adotados.

(57) Embora a *Data (Use and Access) Act* tenha assim alterado o quadro para a tomada de decisões automatizadas, é importante notar que, no âmbito do quadro jurídico do Reino Unido, as decisões automatizadas continuam a estar sujeitas às principais garantias que exigem o direito de obter intervenção humana em todos os casos de decisões significativas baseadas exclusivamente no tratamento automatizado, ou seja, com base no tratamento de dados pessoais sensíveis e não sensíveis ([83]). Além disso, como a Comissão observou em anteriores decisões de

([76]) Artigo 22B do RGPD do Reino Unido, na redação que lhe foi dada pela *section* 80(1) da *Data (Use and Access) Act*.
([77]) Artigo 22A do RGPD do Reino Unido, na redação que lhe foi dada pela *section* 80(1) da *Data (Use and Access) Act*.
([78]) Artigo 22C do RGPD do Reino Unido, na redação que lhe foi dada pela *section* 80(1) da *Data (Use and Access) Act*.
([79]) Artigo 22D do RGPD do Reino Unido, na redação que lhe foi dada pela *section* 80(1) da *Data (Use and Access) Act*. Qualquer regulamentação adotada no âmbito destes poderes está sujeita ao procedimento de resolução positiva, assegurando o controlo parlamentar. Os regulamentos não podem alterar os requisitos previstos no artigo 22C.
([80]) *Section* 182(2) da DPA 2018.
([81]) Artigo 22D(4) do RGPD do Reino Unido.
([82]) Artigo 22D(5) do RGPD do Reino Unido.
([83]) Artigo 22C(2) do RGPD do Reino Unido, na redação que lhe foi dada pela *section* 80(1) da *Data (Use and Access) Act*.

adequação ([84]), as regras específicas em matéria de decisões automatizadas no RGPD do Reino Unido não são suscetíveis de afetar o nível de proteção dos dados pessoais transferidos da União para o Reino Unido. No que se refere aos dados pessoais recolhidos na União, qualquer decisão baseada num tratamento automatizado será, regra geral, tomada pelo responsável pelo tratamento na União (que tem uma relação direta com o titular dos dados em causa), estando, por conseguinte, sujeita às normas do Regulamento (UE) 2016/679.

2.3. **Supervisão e aplicação**

2.3.1. *Supervisão independente*

(58) No Reino Unido, a supervisão e o controlo do cumprimento do quadro de proteção de dados continuam a ser efetuadas por uma autoridade independente de supervisão da proteção de dados, como avaliado nos considerandos 85 a 91 da Decisão de Execução (UE) 2021/1772. A *Data (Use and Access) Act* reforma a estrutura de governação desta autoridade através da criação de uma entidade institucional, a Comissão para a Informação, que irá substituir o ICO, o qual foi estruturado como uma sociedade individual.

(59) Mais especificamente, uma vez aplicadas, as medidas de governação estabelecidas na *Data (Use and Access) Act* resultarão na extinção do Gabinete do Comissário para a Informação e na transferência das funções, do pessoal e dos bens do ICO para o novo organismo, a Comissão para a Informação. A Comissão para a Informação é composta por membros executivos e não executivos ([85]). A lei prevê igualmente que o comissário para a informação assuma a função de presidente da Comissão para a Informação, que é um dos membros não executivos ([86]). A *Data (Use and Access) Act* prevê ainda que, na medida em que tal seja adequado em consequência da transferência de funções, as referências ao comissário para a informação em todos os atos ou outros documentos (sempre que aprovados ou apresentados) devem ser consideradas referências à Comissão para a Informação. Para desempenhar as suas funções, a Comissão pode criar comités e delegar funções num membro, num funcionário ou num comité da Comissão ([87]), bem como estabelecer disposições a fim de regulamentar o seu procedimento e o procedimento dos comités, nomeadamente no que diz respeito ao quórum e à tomada de decisões por maioria. Estes procedimentos devem ser tornados públicos ([88]).

(60) É importante mencionar que a independência da Comissão para a Informação está sujeita às mesmas garantias, incluindo as respeitantes às regras de nomeação e exoneração do presidente, como as avaliadas nos considerandos 87 a 90 da Decisão de Execução (UE) 2021/1772 ([89]). Aplicam-se proteções semelhantes em relação aos outros membros não executivos da Comissão para a Informação. Em especial, o presidente da Comissão para a Informação é nomeado por Sua Majestade, sob recomendação do ministro da tutela. É selecionado com base no mérito e no seguimento de um concurso justo e aberto ([90]). Os restantes membros não executivos são nomeados pelo ministro da tutela após consulta do presidente. Os candidatos só podem ser nomeados ou recomendados para nomeação se forem selecionados com base no mérito na sequência de um concurso justo e aberto e se o ministro da tutela estiver convicto de que não se encontram em situação de conflito de interesses ([91]). Os membros executivos são funcionários da Comissão para a Informação e exercem as suas funções nos termos e condições determinados pelos membros não executivos ([92]). O diretor executivo é nomeado pelo presidente e por outros membros não executivos na sequência de consultas com o ministro da tutela. As nomeações dos membros executivos estão igualmente sujeitas a uma seleção com base no mérito e num concurso justo e aberto ([93]).

(61) O presidente só pode ser demitido das suas funções por Sua Majestade na sequência de um comunicado de ambas as câmaras do Parlamento e apenas se o ministro da tutela tiver apresentado um relatório à câmara em causa declarando que o ministro da tutela está convicto de que o presidente cometeu uma falta grave, tem um conflito de

([84]) Ver, por exemplo, considerando 94 da Decisão de Execução (UE) 2019/419 e considerando 81 da Decisão de Execução (UE) 2022/254 da Comissão, de 17 de dezembro de 2021, nos termos do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho sobre a adequação do nível de proteção dos dados pessoais assegurado pela República da Coreia no âmbito da Lei relativa à proteção de informações pessoais (JO L 44 de 24.2.2022, p. 1, ELI: http://data.europa.eu/eli/dec_impl/2022/254/oj).

([85]) N.º 3(1) do *schedule* 12A da DPA 2018.

([86]) *Sections* 117, 118, 119 e 120, lidas em conjugação com o *schedule* 14 da *Data (Use and Access) Act*.

([87]) N.ºs 13 e 14 do *schedule* 12A da DPA 2018.

([88]) N.º 16 do *schedule* 12A da DPA 2018.

([89]) Artigo 52.º do RGPD do Reino Unido, bem como *schedule* 12A da DPA 2018, na redação que lhe foi dada pela *section* 114A da *Data (Use and Access) Bill*.

([90]) N.ºs 5(1) e 3(2) do *schedule* 12A da DPA 2018.

([91]) N.ºs 3(2), 5 e 6 do *schedule* 12A da DPA 2018.

([92]) N.º 11 do *schedule* 12A da DPA 2018.

([93]) N.º 5(2) do *schedule* 12A da DPA 2018.

interesses, não cumpriu requisitos específicos de informação relativos a potenciais conflitos de interesses ou é incapaz, inapto ou não disposto a desempenhar as funções de presidente ([94]). Os membros não executivos só podem ser destituídos pelo ministro da tutela se este considerar que estão preenchidas as condições específicas estabelecidas na legislação. Estas incluem conflitos de interesses, faltas graves ou ser incapaz, inapto ou não disposto a desempenhar as suas funções. Em termos de garantias adicionais, o ministro da tutela tem a obrigação de tornar pública essa decisão e de apresentar uma exposição dos motivos da destituição ao membro em causa ([95]).

(62) O principal papel da Comissão para a Informação continuará a ser o controlo e a aplicação do quadro de proteção de dados no Reino Unido «a fim de proteger os direitos e liberdades fundamentais» das pessoas singulares ([96]). No que respeita à função da Comissão para a Informação de assegurar um nível adequado de proteção de dados pessoais, a *Data (Use and Access) Act* exige especificamente que a Comissão para a Informação tenha em conta os interesses dos titulares dos dados, dos responsáveis pelo tratamento e de outros, tenha em conta o interesse público em geral e promova a confiança do público no tratamento de dados pessoais ([97]). Estes objetivos também são mencionados no considerando 7 do Regulamento (UE) 2016/679.

(63) Além disso, a *Data (Use and Access) Act* especifica que a Comissão para a Informação deve ter em consideração a promoção da inovação e da concorrência, a importância da prevenção, investigação, deteção e repressão de infrações penais, a necessidade de salvaguardar a segurança pública e a segurança nacional, bem como as necessidades específicas relacionadas com a proteção das crianças no exercício das suas funções nos termos da legislação relativa à proteção de dados ([98]).A legislação da UE relativa à proteção de dados também reconhece a necessidade de conciliar a proteção dos dados pessoais com vários outros direitos fundamentais e objetivos, como o progresso económico e social, a segurança e a justiça e a liberdade de empresa ([99]).

2.3.2. *Controlo do cumprimento, incluindo sanções*

(64) Os poderes e funções da Comissão para a Informação continuam a corresponder às das autoridades de controlo dos Estados-Membros de acordo com os artigos pertinentes do Regulamento (UE) 2016/679 ([100]), conforme avaliado nos considerandos 91 a 95 da Decisão de Execução (UE) 2021/1772.

(65) A *Data (Use and Access) Act* esclarece quanto ao exercício de alguns desses poderes.

(66) Por um lado, a *Data (Use and Access) Act* clarifica que a Comissão pode exigir «documentos» e «informação» específicos ao utilizar o poder de emissão de notas informativas ([101]). Por outro lado, a *Data (Use and Access) Act* introduz dois novos poderes de investigação para a Comissão para a Informação: um novo poder para exigir um relatório ([102]) e um novo poder para emitir «notificações para entrevista» aos responsáveis pelo tratamento em caso de suspeita de violação do RGPD do Reino Unido ou da DPA 2018 ([103]).

([94]) N.º 7(6) e (7) do *schedule* 12A da DPA 2018.
([95]) N.º 9(6), (7), (8) e (9) do *schedule* 12A da DPA 2018.
([96]) Artigo 51.º do RGPD do Reino Unido.
([97]) *Section* 91 da *Data (Use and Access) Act*, que introduz a *section* 120A da DPA 2018.
([98]) *Section* 91 da *Data (Use and Access) Act*, que introduz a *section* 120B da DPA 2018. A *Data (Use and Access) Act* introduz ainda uma nova *section* 120C na DPA 2018, que exige que a Comissão para a Informação elabore e publique uma estratégia que, entre outros aspetos, reflita a forma como terá em conta as questões acima referidas e a promoção do crescimento económico no exercício das suas funções de regulação.
([99]) Ver especialmente considerandos 2 e 4, bem como o artigo 23.º do Regulamento (UE) 2016/679.
([100]) Artigos 57.º e 58.° do RGPD do Reino Unido.
([101]) *Section* 97 da *Data (Use and Access) Act*, que altera a *section* 142 da DPA 2018. As considerações sobre o impacto da tecnologia e o papel da proteção de dados na criação de confiança na economia digital fazem parte das atividades das entidades reguladoras da proteção de dados, tanto no Reino Unido como na UE. Ver, por exemplo, o Relatório Anual de 2024 do Comité Europeu para a Proteção de Dados, p. 12: O CEPD é um organismo dinâmico e colaborativo que desempenha um papel fundamental para assegurar a aplicação coerente da legislação relativa à proteção de dados em toda a Europa. Do meu ponto de vista, como vice-presidente, considero que se trata de um guardião dos direitos de privacidade das pessoas, que habilmente equilibra as necessidades de inovação e de crescimento económico.
([102]) *Section* 98 da *Data (Use and Access) Act*, que altera a *section* 146 da DPA 2018.
([103]) *Section* 100 da *Data (Use and Access) Act*, que introduz a *section* 148A da DPA 2018.

(67) No que diz respeito ao exercício destes poderes pela Comissão para a Informação, desde a entrada em vigor da Decisão de Execução (UE) 2021/1772, o comissário para a informação tratou cerca de 40 000 queixas de titulares de dados por ano, o que é semelhante ao número de queixas tratadas quando o Reino Unido ainda fazia parte da União e aplicou o Regulamento (UE) 2016/679 ([104]). O ICO também realizou investigações *ex officio* que abrangeram uma vasta gama de questões setoriais e de conformidade, incluindo os direitos dos titulares dos dados ([105]).

(68) Em termos de medidas de verificação do cumprimento, desde a entrada em vigor da Decisão de Execução (UE) 2021/1772, o comissário emitiu 120 repreensões, 32 notificações informativas, 3 notificações de avaliação, 12 notificações de execução, 2 advertências e 12 coimas ([106]). Tal inclui várias coimas financeiras avultadas, impostas ao abrigo do RGPD do Reino Unido e da DPA 2018. Por exemplo, o comissário para a informação emitiu, em abril de 2023, uma coima de 12,7 milhões de libras esterlinas a uma plataforma de redes sociais por utilização abusiva de dados de crianças ([107]). Em março de 2025, foi aplicada uma coima de 3,07 milhões de libras esterlinas a uma empresa de *software* por falhas de segurança que colocaram em risco as informações pessoais de mais de 70 000 pessoas ([108]). Muito recentemente, em junho de 2025, o comissário para a informação aplicou uma coima de 2,31 milhões de libras esterlinas a uma empresa de testes genéticos por não ter aplicado medidas de segurança adequadas para proteger as informações pessoais dos utilizadores do Reino Unido, na sequência de um ciberataque de grande escala em 2023 ([109]).

(69) Desde a adoção da Decisão de Execução (UE) 2021/1772, o Gabinete do Comissário para a Informação também elaborou e publicou um número significativo de orientações, pareceres e outros documentos de orientação, que clarificam a aplicação das regras em matéria de proteção de dados em domínios importantes, como o reconhecimento facial, a equidade na inteligência artificial, os dados das crianças, o *marketing* direto, a videovigilância, o direito de acesso, a transparência na saúde e na assistência social, etc., para diferentes públicos, incluindo pequenas e médias empresas, entidades específicas como escolas, infantários ou pequenas autoridades públicas, bem como para as empresas em geral, o público em geral ou os titulares dos dados ([110]).

3. DESENVOLVIMENTOS PERTINENTES RELATIVAMENTE AO ACESSO E UTILIZAÇÃO DE DADOS PESSOAIS TRANSFERIDOS DA UNIÃO EUROPEIA POR AUTORIDADES PÚBLICAS NO REINO UNIDO

3.1. Quadro jurídico geral

(70) O Reino Unido continua a ser membro do Conselho da Europa, mantém a sua adesão à Convenção Europeia dos Direitos Humanos e a submissão à competência jurisdicional do Tribunal Europeu dos Direitos do Humanos. Por conseguinte, continua sujeito às obrigações consagradas no direito internacional, como descrito nos considerandos 116 a 119 da Decisão de Execução (UE) 2021/1772, que enquadram o seu sistema de acesso governamental aos dados pessoais com base em princípios, garantias e direitos individuais idênticos aos aplicáveis aos 27 Estados-Membros enquanto partes na CEDH e que estão, em grande medida, refletidos na jurisprudência pertinente do Tribunal de Justiça da União Europeia.

(71) A DPA 2018 continua a garantir salvaguardas e direitos específicos no domínio da proteção de dados nos casos em que os dados são tratados pelas autoridades públicas do Reino Unido, incluindo por organismos de aplicação da lei e de segurança nacional, conforme avaliado nos considerandos 121 a 132 da Decisão de Execução (UE) 2021/1772. A *Data (Use and Access) Act* introduziu apenas alterações limitadas e específicas às partes da DPA 2018 que preveem as regras para o tratamento de dados pessoais no contexto da aplicação do direito penal (parte 3 da DPA 2018) e da segurança nacional (parte 4 da DPA 2018).

([104]) Relatórios anuais do comissário para a informação de 2021-2022, 2022-2023 e 2023-2024. Ver também a Decisão de Execução (UE) 2021/1772, considerando 96.

([105]) Relatório anual do comissário para a informação de 2023-2024, p. 41.

([106]) Relatórios anuais do comissário para a informação de 2021-2022, 2022-2023 e 2023-2024.

([107]) Para mais informações sobre estas e mais medidas de controlo do cumprimento, consultar o sítio Web do ICO, disponível na seguinte ligação: https://ico.org.uk/action-weve-taken/enforcement/.

([108]) Mais informação disponível na seguinte ligação: https://ico.org.uk/action-weve-taken/enforcement/2025/03/advanced-computer-software-group-limited/.

([109]) Mais informação disponível na seguinte ligação: https://ico.org.uk/action-weve-taken/enforcement/2025/06/23andme/.

([110]) Disponível na seguinte ligação: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/

(72) Relativamente ao tratamento de dados pessoais efetuado pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou da execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública, a parte 3 da DPA 2018 continua a prever princípios, direitos e obrigações semelhantes aos previstos na Diretiva (UE) 2016/680 ([111]).

(73) Especificamente, na mesma data da presente decisão, a Comissão adotou uma decisão com base no artigo 36.º, n.º 3, da Diretiva (UE) 2016/680, e concluiu que o regime de proteção de dados aplicável ao tratamento efetuado pelas autoridades do Reino Unido responsáveis pela aplicação da lei para efeitos de aplicação do direito criminal continua a assegurar um nível de proteção essencialmente equivalente ao assegurado na Diretiva (UE) 2016/680.

(74) A *Data (Use and Access) Act* alterou e consolidou as isenções existentes na parte 3 da DPA 2018 à disposição das autoridades competentes para efeitos de segurança nacional. A isenção relativa à segurança nacional permite às autoridades competentes não aplicar determinadas disposições da parte 3 da DPA 2018 se for necessária uma isenção dessa disposição para salvaguardar a segurança nacional ([112]). Reflete as isenções relativas à segurança nacional previstas para o tratamento de dados pessoais ao abrigo do RGPD do Reino Unido (previstas na *section* 26 da DPA 2018) e da parte 4 da DPA 2018 (previstas na *section* 110 da DPA 2018).

(75) A isenção relativa à segurança nacional encontra-se sujeita às mesmas limitações e garantias que as isenções ao abrigo do RGPD do Reino Unido e da parte 4 da DPA 2018, conforme analisado nos considerandos 64 a 67 e 126 da Decisão de Execução (UE) 2021/1772. Em especial, a isenção só pode ser aplicada se for exigida, e na medida em que seja exigida, para salvaguardar a segurança nacional. Não se trata de uma isenção geral e deve ser considerada e invocada pelo responsável pelo tratamento caso a caso ([113]). Além disso, qualquer aplicação da isenção deve estar em conformidade com as normas em matéria de direitos humanos (sustentadas pelo *Human Rights Act 1998* e pela Convenção Europeia dos Direitos Humanos) segundo as quais qualquer ingerência nos direitos de privacidade deve ser necessária e proporcionada numa sociedade democrática ([114]). As orientações do ICO sobre a aplicação de isenções relativas à segurança nacional também confirmam esse facto ([115]).

(76) Além disso, com base nas alterações introduzidas pela *Data (Use and Access) Act* ([116]), uma atividade de tratamento específica por parte das autoridades competentes no domínio da aplicação do direito penal pode também ser regida pelas disposições da parte 4 da DPA 2018, a qual habitualmente se aplica apenas ao tratamento de dados pelas autoridades nacionais de segurança.

([111]) A *section* 69 da Data (Use and Access) Act insere na DPA 2018 (enquanto novas *sections* 33(1A) e 40A a definição de consentimento e as condições para invocar o consentimento, como previsto no artigo 4.º, n.º 11, e no artigo 7.º do RGPD do Reino Unido [que refletem as disposições correspondentes do Regulamento (UE) 2016/679], clarificando assim o conceito de consentimento e as condições para recorrer ao consentimento quando utilizado como base jurídica para o tratamento de dados pessoais pelas autoridades competentes para efeitos de aplicação do direito penal. Além disso, a *section* 71(7) e (8) da *Data (Use and Access) Act*, clarifica ligeiramente a redação da *section* 36(1) da DPA 2018. Por último, quando pertinente, as alterações do RGPD do Reino Unido pela *Data (Use and Access) Act*, conforme descrito na *section* 2, também estão refletidas na parte 3 da DPA 2018; ver, por exemplo, a *section* 74(2) a (5) sobre o tratamento sensível, a *section* 76(4) a (6) no que diz respeito aos prazos de resposta aos pedidos do titular dos dados, a *section* 78(2) e (3) no que diz respeito às pesquisas em resposta a pedidos dos titulares dos dados e a *section* 80(3) a (5) sobre as decisões automatizadas.

([112]) *Section* 78A(1) da DPA 2018, na redação que lhe foi dada pela *section* 88 da *Data (Use and Access) Act*. Nos termos da *section* 78A(2) a (4) da DPA 2018, a isenção permite afastar a aplicação dos princípios da proteção de dados (com exceção do princípio da licitude e das condições e garantias do tratamento de dados sensíveis), dos direitos individuais, das obrigações dos responsáveis pelo tratamento e dos subcontratantes no que respeita às violações de dados, de determinadas partes das regras relativas às transferências internacionais de dados e de alguns dos poderes do comissário para a informação relativos ao acesso para a realização de inspeções e à tomada de medidas coercivas.

([113]) Ver *Baker/Secretary of State for the Home Department* [2001] UKIT NSA2 («*Baker/Secretary of State*»).

([114]) Ver também *Guriev/Community Safety Development (United Kingdom) Ltd* [2016] EWHC 643 (QB), n.º 45; *Lin/Commissioner of the Police for the Metropolis* [2015] EWHC 2484 (QB), n.º 80.

([115]) Ver as orientações do ICO sobre a exceção relativa à defesa e à segurança nacional, disponíveis na seguinte ligação: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/exemptions/national-security-and-defence-exemption-a-guide.

([116]) *Sections* 89 a 90 da *Data (Use and Access) Act*.

(77) Embora o regime de proteção de dados para o tratamento de dados para efeitos da segurança nacional seja, por conseguinte, alargado, em determinadas situações, também ao tratamento de dados pelas autoridades responsáveis pela aplicação do direito penal, tal só é o caso em circunstâncias específicas e sob reserva de condições e garantias rigorosas, nomeadamente se i) uma autoridade competente for especificada como «autoridade competente habilitada» em regulamentos adotados pelo ministro da tutela que necessitam de aprovação parlamentar ([117]), e ii) o ministro da tutela designar, mediante aviso, uma atividade de tratamento específica realizada pela autoridade competente habilitada. Importa salientar que essa designação só pode ter lugar se o ministro da tutela considerar que a designação da atividade de tratamento é necessária para efeitos de salvaguarda da segurança nacional, ou seja, quando uma autoridade de aplicação do direito penal atua para fins de segurança nacional, e a atividade de tratamento é realizada pela autoridade competente habilitada como responsável conjunto pelo tratamento com, pelo menos, um serviço de informações ([118]). Como garantias adicionais, o ministro da tutela deve consultar o comissário antes de emitir uma notificação de designação ([119]), o texto da notificação deve, em princípio, ser publicado ([120]) e uma pessoa diretamente afetada por uma notificação de designação pode solicitar um recurso judicial ([121]). Por conseguinte, a presente alteração visa essencialmente clarificar que, quando as autoridades do Reino Unido têm competências no domínio da aplicação da lei e da segurança nacional e tratam dados no contexto destas últimas responsabilidades, pode aplicar-se o regime de proteção de dados para os serviços de segurança nacional.

(78) A parte 4 da DPA 2018 rege o tratamento efetuado pelos serviços de informações do Reino Unido. Continua a estabelecer os principais princípios de proteção de dados, a impor condições ao tratamento de categorias especiais de dados, a prever direitos dos titulares dos dados, a exigir a proteção de dados desde a conceção e a regulamentar as transferências de dados pessoais, como descrito nos considerandos 125 a 132 da Decisão de Execução (UE) 2021/1772.

(79) As alterações a este regime introduzidas pela *Data (Use and Access) Act* são limitadas. No que diz respeito ao direito de acesso dos titulares dos dados previsto na *section* 94 da DPA 2018, a *Data (Use and Access) Act* introduz uma nova *subsection* (2A), esclarecendo que o titular dos dados só tem direito às informações pertinentes contanto que o responsável pelo tratamento possa fornecê-las com base numa pesquisa razoável e proporcionada ([122]). Como explicado no considerando 35, esta alteração enquadra o direito de acesso com base em normas jurídicas estabelecidas que também têm em conta os interesses do titular dos dados. Embora, no domínio das decisões automatizadas, continue a ser proibido que os responsáveis pelo tratamento tomem uma decisão que afete significativamente um titular de dados que se baseie inteiramente no tratamento automatizado de dados pessoais que lhe digam respeito, a menos que tal decisão seja exigida ou autorizada por lei, o titular dos dados tenha dado o seu consentimento para que a decisão seja tomada nessa base ou a decisão seja tomada no contexto de um contrato ([123]); a *Data (Use and Access) Act* introduz na parte 4 da DPA 2018 ([124]) a mesma definição do conceito de «decisões inteiramente baseadas no tratamento automatizado» que consta do artigo 22A do RGPD do Reino Unido e analisada no considerando 53 da presente decisão.

3.2. **Desenvolvimentos pertinentes relativamente ao acesso e utilização pelas autoridades públicas do Reino Unido para efeitos de aplicação do direito penal**

(80) O direito do Reino Unido continua a impor uma série de limitações importantes ao acesso e à utilização de dados pessoais para efeitos de aplicação da lei e prevê mecanismos de recurso e supervisão neste domínio, conforme avaliado nos considerandos 134 a 174 da Decisão de Execução (UE) 2021/1772.

([117]) *Section* 82(A1), (2A) e (4) da DPA 2018, na redação que lhe foi dada pela *section* 89(2) da *Data (Use and Access) Act*.

([118]) *Section* 82A(1) e (2), na redação que lhe foi dada pela *section* 89(3) da *Data (Use and Access) Act*. Como garantias adicionais, o ministro da tutela deve consultar o comissário antes de emitir uma notificação de designação [ver nova *section* 82A(8) da DPA 2018], o texto da notificação deve, em princípio, ser publicado [ver nova *section* 82D (1), sob reserva das isenções estabelecidas na nova *section* 82D(3) da DPA 2018], e uma pessoa diretamente afetada por uma notificação de designação pode solicitar um recurso judicial (ver nova *section* 82E da DPA 2018).

([119]) *Section* 82A(8) da DPA 2018.

([120]) *Section* 82D(1), sob reserva das isenções estabelecidas na nova *section* 82D(3) da DPA 2018.

([121]) *Section* 82E da DPA 2018.

([122]) *Section* 78(4) da *Data (Use and Access) Act*.

([123]) *Section* 96 da DPA 2018.

([124]) Nos termos da nova *section* 96(4) da DPA 2018, uma decisão baseia-se num tratamento inteiramente automatizado se o processo de decisão não incluir a oportunidade de um ser humano aceitar, rejeitar ou influenciar a decisão. Ver *section* 80(4)(c) da *Data (Use and Access) Act*.

3.2.1. *Bases jurídicas e limitações/garantias aplicáveis*

(81) A recolha de dados pessoais junto de operadores de empresas no Reino Unido para efeitos de aplicação do direito penal continua a ser permitida na ordem jurídica do Reino Unido com base em mandados de busca e ordens de entrega, sob reserva das condições e garantias descritas nos considerandos 135 a 138 da Decisão de Execução (UE) 2021/1772.

(82) Além disso, a *National Security Act 2023* [Lei de 2023 relativa à Segurança Nacional] ([125]), que visa combater as ameaças à segurança nacional através da espionagem, da sabotagem e das pessoas que atuam por conta de potências estrangeiras, investiu a polícia do Reino Unido de novos poderes de entrada, busca e apreensão, incluindo a possibilidade de obter dados pessoais, sempre que existam motivos razoáveis para suspeitar que serão obtidos elementos suscetíveis de constituir prova de que uma das infrações mais graves ou uma das atividades das potências estrangeiras que constituam ameaças, nos termos da *National Security Act de 2023*, foi ou está prestes a ser cometida ([126]). Estes poderes estão sujeitos a condições e garantias semelhantes às condições e garantias avaliadas na Decisão de Execução (UE) 2021/1772 relativamente aos poderes existentes na altura. Em especial, a sua utilização deve ser autorizada através de um mandado, de uma ordem de entrega ou de uma ordem de explicação emitida por uma autoridade judicial independente, a pedido do agente responsável pela investigação ([127]). Existem proteções específicas para material confidencial, como material jornalístico e objetos sujeitos ao sigilo dos advogados ([128]). Do mesmo modo, a emissão de ordens de divulgação ([129]), de ordens de informação dos clientes ([130]) e de ordens de controlo de contas ([131]) também criadas pela *National Security Act 2023* deve ser autorizada por um juiz, a pedido de um funcionário competente, e está sujeita a condições e garantias específicas, nomeadamente que a decisão seja solicitada relativamente a uma pessoa específica, para efeitos de uma investigação sobre a atividade de ameaça de potência estrangeira, que a ordem melhore a eficácia da investigação e que não seja utilizada para obter informações protegidas pela confidencialidade ou de outra forma excluídas, como material jornalístico e determinados registos de saúde ([132]).

(83) Como descrito nos considerandos 139 a 141 da Decisão de Execução (UE) 2021/1772, no quadro jurídico do Reino Unido, determinadas autoridades responsáveis pela aplicação da lei, por exemplo a *National Crime Agency* ou o *Metropolitan Police Service* também podem utilizar poderes de investigação específicos previstos no *Investigatory Powers Act 2016* [Lei de 2016 relativa aos Poderes de Investigação (IPA 2016)] ([133]) para efeitos de prevenção ou deteção de criminalidade grave. Os poderes de investigação específicos a que essas autoridades responsáveis pela aplicação da lei podem recorrer são os seguintes: interceções direcionadas (parte 2 da IPA 2016), aquisição de dados de comunicações (parte 3 da IPA 2016) e interferência direcionada em equipamentos (parte 5 da IPA 2016). Se forem emitidas notificações de conservação pelo ministro da tutela ao abrigo da parte 4 da IPA 2016, as autoridades de aplicação da lei podem também tirar partido do acesso aos dados de comunicações conservados recorrendo aos poderes de aquisição de dados de comunicações previstos na parte 3 da IPA 2016.

([125]) Disponível na seguinte ligação: https://www.legislation.gov.uk/ukpga/2023/32/contents/enacted.

([126]) *Schedule* 2 da *National Security Act 2023*. As infrações pertinentes no âmbito da *National Security Act 2023* são, por exemplo, a obtenção ou divulgação de informações protegidas (*section* 1), a obtenção ou divulgação de segredos comerciais (*section* 3), a assistência a um serviço de informações externo (*section* 4), sabotagem (*section* 12) ou a prática de comportamentos específicos proibidos por conta de uma potência estrangeira com a intenção de criar um efeito de ingerência (*section* 13).

([127]) Ver n.os 2(1), 3(1), 4(1) e 10(1) do *schedule* 2 da *National Security Act 2023*.

([128]) Ver n.os 2(4)(b), 3(4)5(b) e (c), 4(4)(b) e (c), e 10(1), do *schedule* 2 da *National Security Act 2023*.

([129]) Através de ordens de divulgação, nos termos do *schedule* 3 da *National Security Act 2023*, um funcionário pode notificar uma pessoa da obrigação de fornecer informações, apresentar documentos e/ou a responder a perguntas pertinentes no âmbito de uma investigação destinada a identificar bens relacionados com uma atividade de ameaça de potência estrangeira, incluindo a circulação ou a utilização dos bens.

([130]) Através de ordens de informação do cliente, nos termos do *schedule* 4 da *National Security Act 2023*, um funcionário pode notificar uma instituição financeira da obrigação de fornecer quaisquer informações sobre o cliente relativas a uma determinada pessoa.

([131]) Através de ordens de controlo de contas, nos termos do *schedule* 5, uma instituição financeira pode ser obrigada a fornecer a um funcionário as informações especificadas na ordem durante o período e da forma especificados na ordem, período que não pode exceder 90 dias.

([132]) *Schedule* 3, n.º 2(1), *schedule* 4, n.º 1, *schedule* 5, n.º 1, da *National Security Act 2023*.

([133]) A *Investigatory Powers Act 2016* (ver https://www.legislation.gov.uk/ukpga/2016/25/contents/enacted) substituiu diferentes leis relativas à interceção das comunicações, à interferência com os equipamentos e à aquisição de dados de comunicações, em particular a parte I do RIPA 2000, que estabeleceu o quadro jurídico geral anterior para a utilização dos poderes de investigação pelas autoridades de aplicação da lei e de segurança nacional.

(84) Desde a adoção da Decisão de Execução (UE) 2021/1772, a IPA 2016, em conjunto com o *Regulation of Investigatory Powers Act 2000* [Lei de 2000 relativa ao Regulamento dos Poderes de Investigação (RIPA)] da Inglaterra, do País de Gales e da Irlanda do Norte e o *Regulation of Investigatory Powers (Scotland) Act 2000* [Lei de 2000 relativa ao Regulamento dos Poderes de Investigação (Escócia) (RIPSA)] da Escócia, continuam a apresentar a base jurídica e a estabelecer as limitações e as garantias aplicáveis para a utilização desses poderes, conforme descrito na Decisão de Execução (UE) 2021/1772. É importante salientar que o quadro jurídico continua a exigir que, de modo a exercer estes poderes, as autoridades precisam de obter um mandado ([134]) emitido por uma autoridade competente ([135]) e aprovado por um comissário judicial independente ([136]) [o chamado procedimento «double-lock» (dupla segurança)]. A obtenção desse mandado continua a estar sujeita a um teste de necessidade e proporcionalidade ([137]).

(85) Ao mesmo tempo, desde a adoção da Decisão de Execução (UE) 2021/1772, a *Investigatory Powers (Amendment) Act 2024* [Lei de 2024 relativa aos poderes de investigação (alteração)], que recebeu a aprovação real em abril de 2024, alterou determinados elementos específicos da IPA 2016 ([138]). Uma vez que estas alterações e outros desenvolvimentos pertinentes estão relacionados com as condições, limitações e garantias em torno da utilização dos poderes específicos de investigação, acima referidos, pelas autoridades públicas do Reino Unido para efeitos de aplicação do direito penal, como avaliado nos considerandos 177 a 215 da Decisão de Execução (UE) 2021/1772, as mesmas são avaliadas nos números seguintes. No que diz respeito aos elementos do quadro do Reino Unido que não foram alterados pela referida lei ou afetados por outros desenvolvimentos pertinentes, a análise efetuada na Decisão de Execução (UE) 2021/1772 continua a ser válida.

(86) No que diz respeito à aquisição e conservação específicas de dados de comunicações ([139]), mantêm-se em vigor as condições e garantias que regem estes poderes, como avaliadas na Decisão de Execução (UE) 2021/1772. A *Investigatory Powers (Amendment) Act 2024* clarificou as garantias existentes, introduzindo na *section* 11 da IPA 2016 (que cria uma infração pela obtenção ilícita de dados de comunicações de um operador de telecomunicações) uma lista de exemplos do que se entende por «autoridade legal» nessa disposição ([140]). Além disso, a *Investigatory Powers (Amendment) Act 2024* clarificou ainda mais a definição de dados de comunicações constante da *section* 261 da IPA 2016, especificando explicitamente que os dados do assinante podem ser considerados dados de comunicações ([141]).

([134]) A parte 2, capítulo 2, do IPA 2016 estabelece um número limitado de casos em que as interceções podem ser realizadas sem um mandado. Tal inclui: a interceção com o conhecimento do remetente ou do destinatário, interceção para efeitos administrativos ou de execução, interceção realizada em determinadas instituições (prisões, hospitais psiquiátricos e centros de detenção de imigrantes), bem como interceção efetuada em conformidade com um acordo internacional pertinente.

([135]) Ao abrigo do IPA 2016, na maioria dos casos, a autoridade que emite os mandados é o ministro da tutela, ao passo que os ministros escoceses estão habilitados a emitir mandados de interceção direcionada, mandados de assistência mútua e mandados de interferências específicas com os equipamentos nos casos em que as pessoas ou as instalações que serão intercetadas e os equipamentos que serão alvo de interferência estão localizados na Escócia (ver as *sections* 22 e 103 da IPA 2016). No caso das interferências específicas com os equipamentos, um responsável de aplicação da lei (descrito na parte 1 e na parte 2 do *schedule* 6 da IPA 2016) pode emitir um mandado de acordo com as condições estabelecidas na *section* 106 da IPA 2016.

([136]) Os comissários judiciais auxiliam o comissário para os poderes de investigação (IPC), um organismo independente que exerce funções de supervisão, na utilização dos poderes de investigação pelas agências de informações.

([137]) Ver especificamente as *sections* 19 e 23 da IPA 2016.

([138]) Disponível na seguinte ligação: https://www.legislation.gov.uk/ukpga/2024/9/contents/2025-04-25.

([139]) A expressão «dados de comunicações» abrange o «quem», o «quando», o «onde» e o «como» de uma comunicação, mas não o conteúdo, ou seja, o que foi dito ou escrito. Os dados das comunicações podem incluir a hora e a duração da comunicação, o número ou o endereço de correio eletrónico do remetente e do destinatário e, por vezes, a localização dos dispositivos a partir dos quais as telecomunicações foram efetuadas; ver *section* 261(5) da IPA 2016. A IPA 2016 permite que o ministro da tutela exija que os operadores de telecomunicações conservem dados de comunicações para finalidades de acesso específico por parte de uma série de autoridades públicas, incluindo serviços responsáveis pela aplicação da lei e serviços de informações. A parte 4 da IPA 2016 prevê a conservação de dados de comunicações, enquanto a parte 3 prevê a aquisição direcionada de dados de comunicações. Na parte 3 e na parte 4 da IPA 2016, estabelecem-se igualmente limitações específicas à utilização destes poderes e preveem-se garantias específicas.

([140]) Por exemplo, quando a pessoa em causa obtém os dados de comunicações no exercício de um poder legal da autoridade pública competente ou quando os dados de comunicações são obtidos em conformidade com uma decisão judicial ou outra autorização judicial. *Section* 11 (3A) da IPA 2016, na redação que lhe foi dada pela *section* 12 (3) da *Investigatory Powers (Amendment) Act 2024*.

([141]) *Section* 261(5A) e (5B), na redação que lhe foi dada pela *section* 13(3) da *Investigatory Powers (Amendment) Act 2024*.

(87) A emissão de notificações que exijam a conservação de dados de comunicações ([142]) continua sujeita a limitações e garantias, como descrito nos considerandos 208 e 209 da Decisão de Execução (UE) 2021/1772, especialmente os requisitos de necessidade e proporcionalidade e a aprovação por um comissário judicial independente. Embora a *Investigatory Powers (Amendment) Act 2024* tenha introduzido a possibilidade de renovar essas notificações, qualquer renovação está sujeita às mesmas condições de necessidade, proporcionalidade e aprovação pelo comissário judicial ([143]).

(88) No que respeita aos dados de comunicações, a *Investigatory Powers (Amendment) Act 2024* também alterou a definição de operador de telecomunicações, ou seja, os possíveis destinatários de uma notificação de conservação. Esta definição passa agora a incluir qualquer pessoa que «controle ou forneça um sistema de telecomunicações que i) não esteja (total ou parcialmente) no Reino Unido nem seja controlado a partir do Reino Unido e ii) seja utilizado por outra pessoa para oferecer ou prestar um serviço de telecomunicações a pessoas no Reino Unido» ([144]). Importa salientar que a definição alterada continua a exigir sempre uma ligação estreita com o mercado do Reino Unido. Por conseguinte, a alteração esclarece que as grandes empresas com estruturas empresariais complexas são abrangidas na sua totalidade pela IPA 2016, sem alargar o âmbito de aplicação da definição aos prestadores de serviços de telecomunicações não dirigidos a pessoas no Reino Unido. Este entendimento é igualmente confirmado pelas *Explanatory Notes on the Investigatory Powers (Amendment) Act 2024*, que indicam que a alteração não se destina a incluir outras empresas no âmbito dos poderes relevantes ao abrigo da IPA 2016 ([145]), mas tem essencialmente uma função de clarificação.

(89) Por último, o *Investigatory Powers (Amendment) Act 2024* introduziu algumas alterações específicas ao procedimento de emissão de mandados, inclusive relativamente à interceção direcionada e à interferência específica com os equipamentos, ou seja, poderes que também podem ser utilizados por autoridades responsáveis pela aplicação da lei específicas no Reino Unido para efeitos de prevenção ou deteção de criminalidade grave. As alterações dizem apenas respeito à situação específica em que estes poderes são utilizados para obter comunicações ou informações privadas sobre uma pessoa que é membro de uma legislatura pertinente ([146]). Embora os mandados relativos à interceção direcionada e à interferência com os equipamentos possam normalmente ser emitidos pelo ministro da tutela e sejam aprovados por um comissário judicial [ver considerandos 186 a 196 e 210 a 215 da Decisão de Execução (UE) 2021/1772], as *sections* 26 e 111 da IPA exigem, além disso, a aprovação do primeiro-ministro quando o mandado diz respeito a um deputado ou a outra legislatura pertinente [o chamado procedimento de «triple-lock» (tripla segurança)]. A *Investigatory Powers (Amendment) Act 2024* permite agora ao primeiro-ministro nomear cinco ministros habilitados a exercer o poder daquele de autorizar esses mandados, desde que a necessidade de autorização seja urgente e o primeiro-ministro não possa autorizá-la devido a incapacidade médica ou à falta de acesso a comunicações seguras. Importa salientar que as limitações e garantias no que diz respeito à emissão desses mandados, como descritas nos considerandos acima referidos da Decisão de Execução (UE) 2021/1772, continuam em vigor.

3.2.2. *Utilização adicional das informações recolhidas*

(90) A partilha de dados por uma autoridade de aplicação da lei com outra autoridade para outros fins que não aqueles para os quais foram inicialmente recolhidos (a chamada «transferência subsequente») continua a estar sujeita às condições avaliadas nos considerandos 142 a 156 da Decisão de Execução (UE) 2021/1772.

([142]) A emissão de tais notificações de conservação, em conformidade com as *sections* 87 a 89 da IPA 2016, visa garantir que os operadores de telecomunicações conservam, por um período máximo de 12 meses, dados de comunicações relevantes que, de outro modo, seriam apagados quando deixassem de ser necessários para fins comerciais. Os dados conservados devem permanecer disponíveis durante o período necessário, caso uma autoridade pública tenha posteriormente de os obter ao abrigo de uma autorização para uma aquisição direcionada de dados de comunicações, prevista na parte 3 da IPA 2016.

([143]) *Section* 94A da IPA 2016, na redação que lhe foi dada pela *section* 20 (4) da *Investigatory Powers (Amendment) Act 2024*.

([144]) *Section* 261(10)(c) da IPA 2016, na redação que lhe foi dada pela *section* 19 da *Investigatory Powers (Amendment) Act 2024*.

([145]) *Explanatory Notes on the Investigatory Powers (Amendment) Act 2024*, n.º 359, disponível na seguinte ligação: https://www.legislation.gov.uk/ukpga/2024/9/pdfs/ukpgaen_20240009_en.pdf.

([146]) Ver *sections* 26 e 111 da IPA 2016.

(91) No que diz respeito à situação específica das transferências ulteriores do Reino Unido para os Estados Unidos, o *Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime* (*UK-US Agreement*) [Acordo entre o Governo do Reino Unido da Grã-Bretanha e da Irlanda do Norte e o Governo dos Estados Unidos da América relativo ao acesso aos dados eletrónicos para efeitos de combate à criminalidade grave (Acordo RU-EUA)] ([147]), foi celebrado em outubro de 2019, entrou em vigor e foi aplicado a partir de outubro de 2022. Ao abrigo do Acordo RU-EUA, os dados transferidos da UE para os prestadores de serviços no Reino Unido podem ser sujeitos a ordens para a produção de elementos de prova emitidos pelas autoridades responsáveis pela aplicação da lei competentes dos EUA e aplicáveis no Reino Unido.

(92) Mais importante ainda, continuam a aplicar-se as condições e garantias ao abrigo das quais essas ordens podem ser emitidas e executadas, como avaliado no considerando 154 da Decisão de Execução (UE) 2021/1772. Em especial, os dados obtidos no âmbito do acordo beneficiam de proteções equivalentes às garantias específicas previstas no chamado «Acordo-Quadro UE-EUA» ([148]), todas elas incorporadas no Acordo RU-EUA por remissão, com as devidas adaptações ([149]).

(93) Desde a adoção da Decisão de Execução (UE) 2021/1772, o Reino Unido explicou que esclareceu, incluindo através do diálogo com as partes relevantes no contexto da execução do Acordo RU-EUA, a forma como as garantias específicas do Acordo-Quadro que foram concebidas para um contexto de cooperação na aplicação da lei são adaptadas e aplicadas às transferências específicas abrangidas pelo Acordo RU-EUA. Em especial, o Reino Unido explicou que as disposições do Acordo-Quadro que preveem um papel para a autoridade competente relevante (que não existe numa situação de cooperação direta entre um prestador de serviços do Reino Unido e uma autoridade responsável pela aplicação da lei nos EUA) são interpretadas *mutatis mutandis* no sentido de se referirem à autoridade designada (como definida no Acordo RU-EUA) ([150]) da Parte em causa.

(94) Por exemplo, no que se refere à notificação de um incidente de segurança da informação nos termos do artigo 10.º do Acordo-Quadro UE-EUA, que exige uma notificação à autoridade competente que procede à transferência, o Reino Unido explicou que esta disposição é aplicada *mutatis mutandis* para significar que a notificação deve ser feita à autoridade designada da Parte a partir da qual os dados foram transferidos.

(95) No que diz respeito à autorização da autoridade competente que procede à transferência antes de qualquer transferência ulterior de informações pessoais nos termos do artigo 7.º do Acordo-Quadro, o Reino Unido esclareceu que aplicará essa disposição *mutatis mutandis*, de modo a significar que a autoridade designada da Parte a partir da qual os dados foram transferidos terá de autorizar qualquer transferência posterior.

(96) No que diz respeito às obrigações decorrentes do artigo 8.º do Acordo-Quadro relativo à manutenção da qualidade e integridade das informações, uma interpretação *mutatis mutandis* da disposição tornaria a autoridade designada da Parte que recebe os dados responsável pela ligação com o prestador que transferiu os dados em caso de problemas relacionados com a qualidade e integridade dos dados.

([147]) *Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime*, disponível na seguinte ligação: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/836969/CS_USA_6.2019_Agreement_between_the_United_Kingdom_and_the_USA_on_Access_to_Electronic_Data_for_the_Purpose_of_Countering_Serious_Crime.pdf.

([148]) Acordo entre os Estados Unidos da América e a União Europeia sobre a proteção dos dados pessoais no âmbito da prevenção, investigação, deteção e repressão de infrações penais (JO L 336 de 10.12.2016, p. 3, ELI: http://data.europa.eu/eli/agree_internation/2016/2220/oj).

([149]) Artigo 9.º, n.º 1, do acordo.

([150]) Segundo o artigo 1.º, n.º 8, do Acordo RU-EUA, entende-se por «autoridade designada» a entidade pública designada, no Reino Unido, pelo ministro da Administração Interna e, nos Estados Unidos, pelo procurador-geral.

(97) Em matéria de recurso judicial, o Reino Unido salientou que as transferências ao abrigo do Acordo RU-EUA envolverão sempre a autoridade designada de cada Parte. Se os EUA forem a Parte que recebe dados de prestadores de serviços no Reino Unido, o Ministério da Justiça dos EUA atuará como autoridade designada. Por conseguinte, de acordo com a interpretação do Reino Unido, em cada pedido emitido com base no Acordo RU-EUA, o Ministério da Justiça, enquanto autoridade federal designada ao abrigo da *Judicial Redress Act* [Lei relativa ao Recurso Judicial] dos EUA, estará envolvido, podendo, por conseguinte, ser interposto recurso judicial contra o Ministério da Justiça, em conformidade com o artigo 19.º do Acordo-Quadro. Além disso, o Reino Unido confirmou aos serviços da Comissão que o *Judicial Redress Act* não é o único mecanismo que permite procurar reparação. Em função das circunstâncias e do contexto do caso específico, outras leis aplicáveis dos EUA preveem vias alternativas de recurso judicial.

3.2.3. *Supervisão e vias de recurso*

(98) Em função dos poderes utilizados pelas autoridades competentes no tratamento de dados pessoais para fins de aplicação da lei (ao abrigo da DPA 2018 ou da IPA 2016), diferentes organismos continuam a assegurar a supervisão da utilização desses poderes, como avaliado nos considerandos 158 a 174 da Decisão de Execução (UE) 2021/1772, e continuam a estar disponíveis vias de recurso ao abrigo da parte 3 da DPA 2018, da IPA 2016 e da *Human Rights Act 1998*, como avaliado nos considerandos 250 a 269 da Decisão de Execução (UE) 2021/1772.

(99) No que diz respeito à supervisão da parte 3 da DPA 2018, as funções e os poderes da Comissão para a Informação são avaliados nos considerandos 158 a 160 e 162 da Decisão de Execução (UE) 2021/1772, sob reserva das alterações introduzidas pela *Data (Use and Access) Act* descritas nas secções 2.3.1 e 2.3.2 da presente decisão.

(100) Em termos da aplicação destes poderes, desde a adoção da Decisão de Execução (UE) 2021/1772, o comissário para a informação tratou várias reclamações ([151]) e realizou várias investigações, além de ter tomado medidas de controlo do cumprimento no que diz respeito ao tratamento de dados pelas autoridades responsáveis pela aplicação da lei. Entre 2021 e 2025, o comissário para a informação realizou investigações e emitiu reprimendas a vários organismos de polícia por diferentes incumprimentos das suas obrigações relativas à proteção de dados, por exemplo, na resposta a pedidos de acesso a dados, na aplicação de medidas de segurança para dados de videovigilância, no tratamento de registos criminais confidenciais, na fusão de dados de diferentes pessoas ou na divulgação de dados pessoais a terceiros ([152]). O comissário para a informação também emitiu orientações, pareceres e documentos de orientação, por exemplo sobre o direito de acesso ou sobre a forma de tratar pedidos manifestamente infundados ou excessivos de acordo com a parte 3 da DPA 2018 ([153]).

(101) No que diz respeito à utilização dos poderes de investigação ao abrigo da IPA 2016, a supervisão independente e judicial continua a ser assegurada pelo comissário para os poderes de investigação (IPC), assistido por outros comissários judiciais, coletivamente designados comissários judiciais ([154]). Nesta matéria, a *Investigatory Powers (Amendments) Act 2024* introduziu apenas alterações limitadas e específicas, que não afetam a independência, as funções e os poderes dos comissários judiciais, mas visam reforçar o funcionamento na prática do regime de supervisão existente, especialmente através da introdução de IPC adjuntos nos quais os IPC podem delegar poderes específicos quando estes não puderem ou não estiverem disponíveis para desempenhar as suas funções. Esses IPC adjuntos devem ser comissários judiciais e são nomeados pelo IPC ([155]).

([151]) Por exemplo, em 2023-24, a Comissão para a Informação recebeu 1 890 reclamações com base no RGPD e/ou na DPA 2018 relativas a organizações dos subsetores «Autoridade Policial», «Forças Policiais» e «Comissários da Polícia». Ver também *Information Commissioner's Annual Report and Financial Statements 2023-24* [não traduzido para português], disponível na seguinte ligação: https://ico.org.uk/media2/migrated/4030348/annual-report-2023-24.pdf.

([152]) Mais informação disponível na seguinte ligação: https://ico.org.uk/action-weve-taken/enforcement/?ensector=criminal-justice.

([153]) Disponível na seguinte ligação: https://ico.org.uk/for-organisations/law-enforcement/the-right-of-access-part-3-of-the-dpa-2018/ and https://ico.org.uk/for-organisations/law-enforcement/guide-to-le-processing/individual-rights/manifestly-unfounded-and-excessive-requests/.

([154]) Ver considerando 250 da Decisão de Execução (UE) 2021/1772.

([155]) *Section* 227 da IPA 2016, na redação que lhe foi dada pela *section* 7 da *Investigatory Powers (Amendment) Act*.

3.3. Desenvolvimentos pertinentes relativamente ao acesso e utilização pelas autoridades públicas do Reino Unido para efeitos de segurança nacional

(102) No que diz respeito aos poderes de investigação exercidos no contexto da segurança nacional, a IPA 2016 continua a proporcionar o quadro jurídico para a utilização desses poderes. Além das alterações relativas aos poderes de investigação específicos que, sob reserva de condições específicas, também podem ser invocadas por determinadas autoridades responsáveis pela aplicação da lei, como descrito nos considerandos 77 a 85 da presente decisão, a *Investigatory Powers (Amendment) Act 2024* também introduziu alterações a um dos poderes previstos na IPA 2016 que pode ser exercido em larga escala.

(103) Mais especificamente, a *Investigatory Powers (Amendment) Act 2024* introduziu na nova parte 7A da IPA 2016 um regime específico para a conservação e análise de um subconjunto específico de conjuntos de dados pessoais em larga escala ([156]), ou seja, para os conjuntos de dados em relação aos quais as pessoas a quem os dados pessoais se referem poderiam não ter uma expectativa razoável de privacidade em relação aos dados, ou apenas uma expectativa reduzida de privacidade ([157]). Compete ao chefe de um serviço de informações decidir se um conjunto de dados pessoais em larga escala faz parte deste subconjunto específico de dados pessoais, com base em todas as circunstâncias, especialmente: i) a natureza dos dados, ii) em que medida os dados foram tornados públicos pelas pessoas singulares, ou em que medida as pessoas deram o seu consentimento para que os dados fossem tornados públicos, iii) se os dados tiverem sido publicados, em que medida foram publicados sob controlo editorial ou por uma pessoa que atue em conformidade com as normas profissionais, iv) se os dados tiverem sido publicados ou estiverem, de outra forma, no domínio público, em que medida os dados são amplamente conhecidos, e v) em que medida os dados já foram utilizados no domínio público ([158]).

(104) É importante salientar que, no que diz respeito à conservação e análise de conjuntos de dados pessoais em larga escala que não se enquadram nesta categoria, ou seja, os que são mais sensíveis e que, consequentemente, implicam uma expectativa razoável de privacidade, o regime avaliado nos considerandos 239 e 240 da Decisão de Execução (UE) 2021/1772 continua em vigor, especialmente a necessidade de um mandado aprovado primeiro pelo ministro da tutela e, em seguida, pelo comissário judicial, sob reserva dos requisitos de necessidade e proporcionalidade da medida, como previsto na parte 7 da IPA 2016 ([159]).

(105) A parte 7A da IPA 2016 prevê dois tipos de autorização: a autorização individual e a autorização por categoria. A conservação, ou a conservação e a análise, de cada conjunto de dados pessoais em larga escala retidos ao abrigo da parte 7A deve ser autorizada ao abrigo de uma destas autorizações. Ambas as autorizações exigem, em princípio ([160]), a autorização do chefe do serviço de informações (ou de uma pessoa que atue em seu nome) e a aprovação de um comissário judicial independente ([161]). As autorizações individuais são concedidas pelo chefe de um serviço de informação, de acordo com as condições previstas na *section* 226B(4) da IPA 2016, e sujeitas à aprovação prévia dos comissários judiciais. O comissário judicial tem de analisar as conclusões da pessoa que concedeu a autorização quanto à aplicação da *section* 226A, isto é, o requisito da expectativa reduzida ou não razoável de privacidade, ao conjunto de dados pessoais em larga escala descrito na autorização ([162]).

([156]) Os mandados de conjuntos de dados pessoais em larga escala emitidos nos termos da *section* 200 da IPA 2016 autorizam os serviços de informações a conservar e examinar conjuntos de dados que contêm dados pessoais relativos a várias pessoas e a natureza do conjunto é tal que a maioria das pessoas não tem interesse para o serviço de informações no exercício das suas funções, e é pouco provável que o venha a ter, que o conjunto é conservado eletronicamente por um serviço de informações e guardado para análise no exercício das suas funções legais; ver também *section* 199 da IPA 2016.

([157]) *Section* 226A(1) da IPA 2016, na redação que lhe foi dada pela *section* 2 da *Investigatory Powers (Amendment) Act 2024*.

([158]) *Section* 226A(3) da IPA 2016, na redação que lhe foi dada pela *section* 2 da *Investigatory Powers (Amendment) Act 2024*.

([159]) A *Investigatory Powers (Amendment) Act 2024* alterou a *section* 213 da IPA 2016 no sentido de que os mandados de conjuntos de dados pessoais em larga escala deixam de produzir efeitos 12 meses após a sua emissão. Anteriormente, esses mandados tinham de ser renovados a cada 6 meses. Ver *section* 3 da *Investigatory Powers (Amendment) Act 2024*.

([160]) As autorizações individuais só podem ser concedidas sem aprovação judicial prévia i) se a pessoa que concede a autorização individual considerar que o conjunto de dados pessoais em larga escala em causa é abrangido por uma autorização por categoria existente ou ii) em caso de urgência; ver *section* 226B(6) da IPA 2016. Neste último caso, a decisão de conceder uma autorização individual urgente tem de ser analisada por um comissário judicial no prazo de três dias úteis a contar da data de emissão; ver *section* 226BC da IPA 2016.

([161]) *Section* 226B(1) da IPA 2016, na redação que lhe foi dada pela *section* 2 da *Investigatory Powers (Amendment) Act*.

([162]) *Section* 226BB(1)(a) da IPA 2016, na redação que lhe foi dada pela *section* 2 da *Investigatory Powers (Amendment) Act 2024*.

(106) As autorizações por categoria autorizam a conservação, ou a conservação e análise, de uma categoria de conjuntos de dados pessoais em larga escala descritos na autorização.

(107) A decisão de conceder autorizações por categoria é tomada pelo chefe do serviço de informação se este considerar que a *section* 226A se aplica a quaisquer conjuntos de dados da categoria e se a decisão de concessão da autorização for aprovada por um comissário judicial independente ([163]). Este último deve analisar se a *section* 226A, isto é, o requisito da expectativa reduzida ou não razoável de privacidade, é aplicável a qualquer conjunto de dados pessoais abrangido pela categoria de conjuntos de dados pessoais descrita na autorização ([164]).

(108) Importa salientar que, ao aprovar uma decisão de concessão de uma autorização individual ou por categoria, o comissário judicial deve «aplicar os mesmos princípios que seriam aplicados por um órgão jurisdicional no âmbito de um pedido de fiscalização jurisdicional» ([165]) e considerar estas questões com um grau de diligência suficiente para assegurar que o comissário judicial cumpre os deveres impostos pela *section* 2 da IPA 2016 (deveres gerais relativos à privacidade) ([166]). Além disso, a emissão de autorizações está sujeita a uma rigorosa supervisão *ex post*, especialmente através da apresentação de relatórios anuais ao ministro da tutela e ao Comité do Parlamento para as Informações e Segurança ([167]) e através de inspeções regulares ao Gabinete do IPC ([168]).

(109) Em termos de desenvolvimentos pertinentes no domínio da supervisão, o Gabinete do IPC publicou relatórios anuais relativos aos anos de 2021, 2022 e 2023, que fornecem estatísticas e informações pormenorizadas sobre a utilização dos poderes de investigação pelos serviços de informações e pelas autoridades responsáveis pela aplicação da lei no Reino Unido ([169]). Os relatórios descrevem também as auditorias e inquéritos do Gabinete, bem como as respetivas conclusões, confirmando que o IPC continua a assegurar a sua muito importante função de supervisão ao abrigo do regime de poderes de investigação do Reino Unido. Por exemplo, em 2023, analisou a necessidade e as justificações da proporcionalidade para a utilização dos poderes de interceção em larga escala [como avaliado nos considerandos 218 a 225 da Decisão de Execução (UE) 2021/1772] pela Sede das Comunicações do Governo (GCHQ), concluindo que uma maioria significativa das declarações foi articulada com uma fundamentação sólida, embora, em alguns casos, a proporcionalidade não tenha sido devidamente expressa. Estas conclusões foram debatidas com a Equipa de Conformidade da GCHQ, que se comprometeu a encomendar formação adicional para sensibilização interna quanto a esta questão ([170]).

(110) Além disso, o *Investigatory Powers Tribunal* (tribunal competente em matéria de investigação) emitiu um relatório público das suas atividades e jurisprudência para o período de 2021 a 2023 ([171]). O relatório revela que o número de processos recebidos pelo *Tribunal* mais do que duplicou desde 2017, tendo sido recebidos mais de 400

([163]) *Section* 226BA da IPA 2016, na redação que lhe foi dada pela *section* 2 da *Investigatory Powers (Amendment) Act*.

([164]) *Section* 226Bb(1)(b) da IPA 2016, na redação que lhe foi dada pela *section* 2 Investigatory Powers (Amendment) Act.

([165]) *Section* 226BB(2)(a) da IPA 2016, na redação que lhe foi dada pela *section* 2 da *Investigatory Powers (Amendment) Act 2024*.

([166]) *Section* 226BB(2)(b) da IPA 2016, na redação que lhe foi dada pela *section* 2 da *Investigatory Powers (Amendment) Act 2024*. De acordo com os deveres gerais relativos à privacidade, conforme previstos na *section* 2 da IPA 2016, a autoridade pública deve ter em conta a) se o que se pretende alcançar através do mandado, autorização ou notificação pode, na medida do razoável, ser alcançado com recurso a outros meios menos intrusivos, b) se o nível de proteção a aplicar em relação a qualquer obtenção de informações por força do mandado, autorização ou notificação é mais elevado devido à especial sensibilidade dessas informações, c) ao interesse público na integridade e segurança de quaisquer outros sistemas de telecomunicações e serviços postais e d) a quaisquer outros aspetos de interesse público na proteção da privacidade.

([167]) *Sections* 226DA e 226DB da IPA 2016, na redação que lhes foi dada pela *section* 2 da *Investigatory Powers (Amendment) Act 2024*.

([168]) Ver *2023 Annual Report of the Investigatory Powers Commissioner* [não traduzido para português], disponível na seguinte ligação: https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/E03270100-HC_603-IPCO-Annual-Report-2023-Web_Accessible.pdf, p.3.

([169]) Todos os relatórios anuais estão disponíveis na seguinte ligação: https://www.ipco.org.uk/publications/annual-reports/.

([170]) Ver parágrafos 6.39 a 6.43 do *Annual Report 2023*, disponível na seguinte ligação: https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/E03270100-HC_603-IPCO-Annual-Report-2023-Web_Accessible.pdf.

([171]) Relatório do *Investigatory Powers Tribunal* para 2021-2023, disponível na seguinte ligação: https://investigatorypowerstribunal.org.uk/wp-content/uploads/2024/11/Investigatory-Powers-Tribunal-Report-2024.pdf.

processos em 2023 ([172]). A maioria das queixas foi apresentada contra os organismos responsáveis pela aplicação da lei, a que se seguiram de perto as autoridades de segurança e informação ([173]). Cumpre salientar que, em 2022 e 2023, o *Tribunal* proferiu decisões em processos recebidos antes de 2021, nos quais concluiu que autoridades públicas do Reino Unido [respetivamente, a *Police Scotland* ([174]), a *Greater Manchester Police* ([175]), a *Surrey Police* ([176]) e o *MI5* e o *Home Secretary* ([177])] tinham atuado de forma ilegal. No que respeita às medidas decretadas, o *Investigatory Powers Tribunal* ordenou, entre outras medidas, a destruição de qualquer material obtido ilegalmente e, num processo, também o pagamento de 12 000 GBP a título de reparação justa pelas violações identificadas. Por conseguinte, o relatório anual confirma que o *Investigatory Powers Tribunal* desempenha efetivamente o seu importante papel na garantia da supervisão e da reparação no domínio da aplicação do direito penal e do acesso a dados pessoais no âmbito da segurança nacional.

(111) O relatório destaca ainda desenvolvimentos importantes, como um acórdão proferido pelo Tribunal Europeu dos Direitos Humanos no qual o Tribunal considerou que as pessoas singulares de qualquer parte do mundo podem intentar uma ação perante o *Investigatory Powers Tribunal* relativa ao funcionamento do regime de interceção em larga escala do Reino Unido quando a conduta em causa tiver ocorrido no Reino Unido e sido praticada por um organismo público do Reino Unido ([178]).

4. **CONCLUSÃO**

(112) A Comissão entende que o RGPD do Reino Unido e a DPA 2018, na redação que lhes foi dada pela *Data (Use and Access) Act*, continuam a assegurar um nível de proteção dos dados pessoais transferidos da União Europeia essencialmente equivalente ao garantido pelo Regulamento (UE) 2016/679.

(113) Além disso, a Comissão considera que os mecanismos de controlo e as vias de recurso previstas na legislação do Reino Unido continuam a permitir, no seu conjunto, identificar e sancionar na prática as violações, proporcionando vias judiciais aos titulares dos dados para ter acesso aos respetivos dados pessoais e, em última instância, requerer a retificação ou o apagamento dos mesmos.

(114) Por último, com base nas informações disponíveis sobre o quadro jurídico do Reino Unido, a Comissão entende que qualquer ingerência das autoridades públicas do Reino Unido nos direitos fundamentais das pessoais singulares, cujos dados pessoais sejam transferidos da União Europeia para o Reino Unido, para fins de interesse público, designadamente, para efeitos de aplicação da lei e de segurança nacional, continua a estar limitada ao estritamente necessário para alcançar o objetivo legítimo em causa, existindo uma proteção jurídica eficaz contra tais ingerências.

(115) Assim, atendendo às constatações efetuadas na presente decisão, deve decidir-se que o Reino Unido continua a garantir um nível adequado de proteção na aceção do artigo 45.º do Regulamento (UE) 2016/679, interpretado em função da Carta dos Direitos Fundamentais da União Europeia.

(116) Esta conclusão baseia-se tanto no regime interno aplicável do Reino Unido, com os seus desenvolvimentos desde a adoção da Decisão de Execução (UE) 2021/1772, como nos seus compromissos internacionais, em particular o facto de o Reino Unido manter a sua adesão à Convenção Europeia dos Direitos Humanos e a submissão à competência jurisdicional do Tribunal Europeu dos Direitos do Humanos. Por conseguinte, a adesão contínua a essas obrigações internacionais é um elemento particularmente importante da avaliação em que se baseia a presente decisão.

([172]) Relatório do *Investigatory Powers Tribunal* para 2021-2023, p. 5.
([173]) Relatório do *Investigatory Powers Tribunal* para 2021-2023, p. 12.
([174]) Wilson/Police Scotland [2022] UKIPTrib 5.
([175]) Pendlebury/Greater Manchester Police [2023] UKIPTrib 2.
([176]) Hill/Metropolitan Police Service e Independent Office For Police Conduct [2022] UKIPTrib 6.
([177]) Liberty & Privacy International/Security Service e Secretary of State for the Home Department [2023] UKIPTrib 1.
([178]) *Wieder e Guarnieri/Reino Unido*, [2023] ECHR 668; ver também o Relatório do *Investigatory Powers Tribunal* para 2021-2023, p. 6.

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

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

(118) Consequentemente, uma decisão de adequação da Comissão adotada nos termos do artigo 45.º, n.º 3, do Regulamento (UE) 2016/679 é vinculativa para todos os organismos dos Estados-Membros aos quais se destina, nomeadamente para as suas autoridades de controlo independentes. Em especial, durante o período de aplicação da Decisão de Execução (UE) 2021/1772, conforme alterada pela presente decisão, as transferências de um responsável pelo tratamento ou de um subcontratante na União Europeia para responsáveis pelo tratamento ou subcontratantes no Reino Unido podem ser efetuadas sem que seja necessária mais nenhuma autorização.

(119) Importa recordar que, nos termos do artigo 58.º, n.º 5, do Regulamento (UE) 2016/679, e conforme explicado pelo Tribunal de Justiça no acórdão *Schrems I* ([179]), se uma autoridade nacional responsável pela proteção de dados colocar em causa, nomeadamente na sequência de uma reclamação, a conformidade de uma decisão de adequação da Comissão com a proteção dos direitos fundamentais à privacidade e à proteção dos dados da pessoa singular, a legislação nacional deve proporcionar-lhe uma via de recurso que lhe permita apresentar tais objeções junto de um tribunal nacional, que poderá ter de proceder a um reenvio prejudicial para o Tribunal de Justiça ([180]).

6. **CONTROLO**

(120) Nos termos do artigo 45.º, n.º 4, do Regulamento (UE) 2016/679, a Comissão deve controlar, de forma continuada, os desenvolvimentos pertinentes no Reino Unido, a fim de avaliar se este ainda assegura um nível de proteção essencialmente equivalente. Este controlo é particularmente importante, uma vez que o Reino Unido irá aplicar e fazer cumprir um regime de proteção de dados alterado. Além disso, o quadro de proteção de dados alterado do Reino Unido habilita o ministro da tutela a especificar melhor este quadro através de legislação derivada. A este respeito, deve ser prestada especial atenção a essas especificações adicionais, bem como à aplicação, na prática, das regras alteradas do Reino Unido em matéria de transferência de dados pessoais para países terceiros; à eficácia do exercício dos direitos individuais, incluindo quaisquer desenvolvimentos pertinentes na legislação e nas práticas a respeito das exceções ou restrições recentemente introduzidas a esses direitos, ao funcionamento do ICO reestruturado, nomeadamente no que se refere à gestão de reclamações e à aplicação de poderes de correção, bem como ao cumprimento das restrições e garantias relativas ao acesso governamental, em especial no que se refere à parte 7A recentemente introduzida da IPA 2016. Entre outros elementos, o controlo da Comissão basear-se-á nos desenvolvimentos da jurisprudência e na supervisão pelo ICO e outros organismos independentes.

(121) A fim de facilitar este controlo, as autoridades do Reino Unido devem informar prontamente a Comissão de qualquer alteração substancial da ordem jurídica do Reino Unido que tenha impacto no quadro jurídico objeto da Decisão de Execução (UE) 2021/1772, conforme alterada pela presente decisão, bem como de qualquer evolução das práticas relacionadas com o tratamento dos dados pessoais avaliadas na Decisão de Execução (UE) 2021/1772, conforme alterada pela presente decisão, tanto no que diz respeito ao tratamento de dados pessoais pelos responsáveis pelo tratamento e subcontratantes ao abrigo do RGPD do Reino Unido, como às restrições e às garantias aplicáveis ao acesso aos dados pessoais pelas autoridades públicas. Tal deverá incluir desenvolvimentos no que diz respeito aos elementos mencionados no considerando 120.

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

([179]) Acórdão *Schrems I*, n.º 65.

([180]) Acórdão *Schrems I*, n.º 65: «A este respeito, incumbe ao legislador nacional prever vias de recurso que permitam à autoridade nacional de controlo em causa invocar as críticas que considera fundadas perante os órgãos jurisdicionais nacionais, para que estes últimos, caso partilhem das dúvidas dessa autoridade quanto à validade da decisão da Comissão, procedam a um reenvio prejudicial para efeitos da apreciação da validade dessa decisão».

(123) Sempre que as informações disponíveis, nomeadamente as resultantes do controlo da Decisão de Execução (UE) 2021/1772, conforme alterada pela presente decisão, ou fornecidas pelas autoridades do Reino Unido ou dos Estados-Membros, revelarem que o nível de proteção conferido pelo Reino Unido pode já não ser adequado, a Comissão deve informar prontamente as autoridades competentes do Reino Unido desse facto e solicitar que sejam adotadas medidas adequadas dentro de um prazo especificado, que não deve exceder os três meses. Se necessário, esse prazo pode ser prorrogado por um período determinado, tendo em conta a natureza da questão em causa e/ /ou das medidas a adotar. Por exemplo, tal procedimento seria desencadeado caso as transferências ulteriores, incluindo com base em novos regulamentos de adequação adotados pelo ministro da tutela ou em acordos internacionais celebrados pelo Reino Unido, deixassem de ser efetuadas ao abrigo de garantias que assegurem a continuidade da proteção na aceção do artigo 44.º do Regulamento (UE) 2016/679.

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

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

(126) Por imperativos de urgência devidamente justificados, a Comissão recorrerá à possibilidade de adotar, em conformidade com o procedimento referido no artigo 93.º, n.º 3, do Regulamento (UE) 2016/679, atos de execução imediatamente aplicáveis que suspendam, revoguem ou alterem a decisão.

7. **AVALIAÇÃO, VIGÊNCIA E RENOVAÇÃO DA PRESENTE DECISÃO**

(127) Por força do artigo 45.º, n.º 3, do Regulamento (UE) 2016/679, e atendendo a que o nível de proteção conferido pelo quadro jurídico do Reino Unido pode vir a alterar-se, a Comissão deve, na sequência da adoção da presente decisão, avaliar periodicamente se as verificações de adequação do nível de proteção assegurado pelo Reino Unido continuam a justificar-se de facto e de direito, tendo em conta os elementos enumerados no artigo 45.º, n.º 2, do Regulamento (UE) 2016/679. Essas avaliações devem ser realizadas, no mínimo, de quatro em quatro anos e devem abranger todos os aspetos do funcionamento da presente decisão, incluindo o funcionamento dos mecanismos de supervisão e execução pertinentes.

(128) Para realizar a avaliação, a Comissão deve reunir com os representantes pertinentes das autoridades do Reino Unido, incluindo com a Comissão para a Informação. Essa reunião deve ser aberta à participação de representantes dos membros do Comité Europeu para a Proteção de Dados. No quadro da avaliação, a Comissão deve solicitar ao Reino Unido que preste informações exaustivas sobre todos os aspetos pertinentes para a verificação de adequação. A Comissão deve também procurar obter explicações sobre quaisquer informações que tenha recebido com relevância para a presente decisão, nomeadamente do CEPD, de autoridades de proteção de dados individuais, de grupos da sociedade civil, de relatórios públicos ou de meios de comunicação social ou de qualquer outra fonte de informação disponível.

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

(130) A Comissão deve igualmente ter em conta que o quadro de proteção de dados avaliado na presente decisão e na Decisão de Execução (UE) 2021/1772 pode continuar a evoluir.

(131) Por conseguinte, convém prever que a presente decisão seja aplicável por um período de seis anos a partir da sua entrada em vigor.

(132) Se, em particular, as informações resultantes do controlo da presente decisão revelarem que as conclusões relativas à adequação do nível de proteção assegurado no Reino Unido continuam a justificar-se de facto e de direito, a Comissão deve, o mais tardar seis meses antes de a presente decisão deixar de ser aplicável, dar início ao procedimento de alteração da presente decisão, prorrogando a sua aplicação no tempo, em princípio, por um período adicional de quatro anos. Qualquer ato de execução que altere a presente decisão deve ser adotado em conformidade com o procedimento referido no artigo 93.º, n.º 2, do Regulamento (UE) 2016/679.

8. **CONSIDERAÇÕES FINAIS**

(133) O Comité Europeu para a Proteção de Dados publicou um parecer ([181]) que foi tido em conta na elaboração da presente decisão.

(134) A medida prevista na presente decisão está em conformidade com o parecer do Comité instituído ao abrigo do artigo 93.º do Regulamento (UE) 2016/679,

(135) A Decisão de Execução (UE) 2021/1772 deve, por conseguinte, ser alterada em conformidade,

ADOTOU A PRESENTE DECISÃO:

Artigo 1.º

É revogado o artigo 1.º, n.º 2, da Decisão de Execução (UE) 2021/1772.

Artigo 2.º

O artigo 4.º da Decisão de Execução (UE) 2021/1772 passa a ter a seguinte redação:

«*Artigo 4.º*

A presente decisão caduca em 27 de dezembro de 2031, a menos que seja prorrogada nos termos do procedimento referido no artigo 93.º, n.º 2, do Regulamento (UE) 2016/679.».

Artigo 3.º

Os destinatários da presente decisão são os Estados-Membros.

Feito em Bruxelas, em 19 de dezembro de 2025.

Pela Comissão
Michael MCGRATH
Membro da Comissão

([181]) Parecer 26/2025 relativo ao Projeto de Decisão de Execução da Comissão Europeia nos termos do Regulamento (UE) 2016/679 sobre a adequação do nível de proteção dos dados pessoais assegurado pelo Reino Unido, disponível na seguinte ligação: https://www.edpb.europa.eu/system/files/2025-10/edpb_opinion_202526_united_kingdom_adequacy_gdpr_en.pdf.