II

(Atos não legislativos)

DECISÕES

REGULAMENTO 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

[notificada com o número C(2021) 4800]

(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) O Regulamento (UE) 2016/679 estabelece as regras relativas à transferência de dados pessoais para países terceiros e organizações internacionais pelos responsáveis pelo tratamento e subcontratantes na União Europeia, na medida em que essa transferência seja abrangida pelo respetivo âmbito de aplicação. As regras relativas às transferências internacionais de dados pessoais são definidas no capítulo V do referido regulamento, mais concretamente nos artigos 44.º a 50.º. Embora a circulação de dados pessoais com origem e destino a países não pertencentes à União Europeia seja essencial para o desenvolvimento da cooperação internacional e do comércio transfronteiriço, é indispensável garantir que o nível de proteção conferido aos dados pessoais na União Europeia não é comprometido por transferências para países terceiros ([2]).

(2) Nos termos do artigo 45.º, n.º 3, do Regulamento (UE) 2016/679, a Comissão pode decidir, através de um ato de execução, que um país terceiro, um território ou um ou mais setores específicos de um país terceiro, ou uma organização internacional, garante um nível de proteção adequado. Nessa condição, as transferências de dados pessoais para um país terceiro podem realizar-se sem que para tal seja necessária mais nenhuma autorização, conforme previsto no artigo 45.º, n.º 1, e no considerando 103 do referido regulamento.

(3) De acordo com o estabelecido no artigo 45.º, n.º 2, do Regulamento (UE) 2016/679, a adoção de uma decisão de adequação deve basear-se numa análise exaustiva da ordem jurídica do país terceiro, que abranja tanto as regras aplicáveis aos importadores de dados como as limitações e garantias relativas ao acesso aos dados pessoais pelas autoridades públicas. Na sua avaliação, a Comissão tem de apurar se o país terceiro em causa garante um nível de proteção «essencialmente equivalente» ao assegurado na União Europeia [considerando 104 do Regulamento (UE) 2016/679]. O critério pelo qual se avalia a «equivalência essencial» é o estabelecido pela legislação da União Europeia, nomeadamente pelo Regulamento (UE) 2016/679, bem como pela jurisprudência do Tribunal de Justiça da União Europeia ([3]). O documento de referência relativo à adequação do Comité Europeu para a Proteção de Dados (CEPD) é também importante nesta matéria ([4]).

([1]) JO L 119 de 4.5.2016, p. 1.
([2]) Ver considerando 101 do Regulamento (UE) 2016/679.
([3]) Ver, mais recentemente, o processo C-311/18, *Facebook Ireland e Schrems* («*Schrems II*»), ECLI:EU:C:2020:559.
([4]) Comité Europeu para a Proteção de Dados, documento de referência relativo à adequação, WP 254 rev. 01, disponível na seguinte ligação: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108

(4) Conforme esclareceu o Tribunal de Justiça da União Europeia, não é exigido um nível de proteção idêntico ([5]). Mais concretamente, os meios a que o país terceiro em causa recorre para proteger os dados pessoais podem ser diferentes dos aplicados na União Europeia, desde que se revelem, na prática, eficazes para assegurar um nível adequado de proteção ([6]). Por conseguinte, para que se verifique a adequação não é necessário 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 sistema estrangeiro consegue, no seu conjunto, garantir o nível de proteção exigido ([7]).

(5) A Comissão procedeu a uma análise cuidadosa da legislação e das práticas do Reino Unido. Com base nas constatações formuladas nos considerandos 8 a 270, a Comissão conclui que o Reino Unido assegura um nível de proteção adequado dos dados pessoais transferidos no âmbito do Regulamento (UE) 2016/679 da União Europeia para o Reino Unido.

(6) Esta conclusão não diz respeito aos 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, do *UK Data Protection Act* (DPA, Lei relativa à proteção de dados do Reino Unido). A validade e a interpretação da isenção relativa à imigração ao abrigo do direito do Reino Unido não são resolvidas 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. Embora reconhecendo que os direitos dos titulares dos dados podem, em princípio, ser limitados para efeitos de controlo da imigração como «um aspeto importante do interesse público», o *Court of Appeal* considerou que a isenção relativa à imigração é, na sua forma atual, incompatível com o direito do Reino Unido, uma vez que a medida legislativa carece de disposições específicas que estabeleçam as garantias enumeradas no artigo 23.º, n.º 2, do Regulamento Geral sobre a Proteção de Dados do Reino Unido (RGPD do Reino Unido) ([8]). Nestas condições, as transferências de dados pessoais da União para o Reino Unido às quais é possível aplicar a isenção relativa à imigração devem ser excluídas do âmbito da presente decisão ([9]). Uma vez corrigida a incompatibilidade com o direito do Reino Unido, a isenção relativa à imigração deve ser reavaliada, bem como a necessidade de manter a limitação do âmbito da presente decisão.

(7) A presente decisão não deve afetar a aplicação direta do Regulamento (UE) 2016/679 às organizações estabelecidas no Reino Unido que preencham as condições relativas ao âmbito de aplicação territorial do referido regulamento, previstas no seu artigo 3.º.

2. **NORMAS APLICÁVEIS AO TRATAMENTO DE DADOS PESSOAIS**

2.1. **Quadro constitucional**

(8) O Reino Unido é uma democracia parlamentar, que tem um monarca constitucional como Chefe de Estado. Possui um parlamento soberano, com supremacia em relação a todas as outras instituições governamentais, um executivo proveniente do parlamento e ao qual presta contas, e um poder judicial independente. O executivo obtém a sua autoridade da capacidade de manter a confiança da Câmara dos Comuns eleita, e presta contas a ambas as câmaras do parlamento, que são responsáveis pelo escrutínio do governo e por debater e aprovar a legislação.

([5]) Processo C-362/14, *Schrems* («*Schrems I*»), ECLI:EU:C:2015:650, n.º 73.

([6]) *Schrems I*, n.º 74.

([7]) 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. 6-7, disponível na seguinte ligação: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017DC0007&from=EN

([8]) *Court of Appeal (Civil Division), Open Rights Group/Secretary of State for the Home Department and Secretary of State for Digital, Culture, Media and Sport* [2021] EWCA Civ 800, n.ºs 53 a 56. O *Court of Appeal* inverteu a decisão do *High Court of Justice* (Tribunal Superior de Justiça) que tinha previamente apreciado a isenção à luz do Regulamento (UE) 2016/679 (em especial, o seu artigo 23.º) e da Carta dos Direitos Fundamentais da União Europeia e considerou a isenção lícita (*Open Rights Group & Anor, R (on the application of f)/Secretary of State for the Home Department & Anor* [2019] EWHC 2562).

([9]) Desde que as condições aplicáveis sejam cumpridas, as transferências para efeitos de controlo da imigração do Reino Unido podem ser efetuadas com base nos mecanismos de transferência previstos nos artigos 46.º a 49.º do Regulamento (EU) 2016/679.

(9) O parlamento do Reino Unido delegou no parlamento escocês, no parlamento do País de Gales (*Senedd Cymru*) e na Assembleia da Irlanda do Norte a responsabilidade de legislar, nos respetivos territórios, sobre matérias internas que não tenha reservado para si próprio. Embora a proteção de dados seja uma matéria reservada, ou seja, a mesma legislação aplica-se a todo o território, existem outros domínios de intervenção pertinentes para a presente decisão que foram delegados. Por exemplo, os sistemas de justiça penal, nomeadamente o policiamento, da Escócia e da Irlanda do Norte são da competência do parlamento Escocês e da Assembleia da Irlanda do Norte, respetivamente. O Reino Unido não possui uma constituição codificada na aceção de um documento constitutivo codificado. Os princípios constitucionais foram surgindo ao longo do tempo, tendo origem, em particular, na jurisprudência e em convenções. O valor constitucional de determinadas leis, nomeadamente a *Magna Carta*, a *Bill of Rights 1689* (Declaração de Direitos de 1689) e o *Human Rights Act 1998* (Lei de 1998 relativa aos Direitos Humanos), foi reconhecido pelos tribunais. Os direitos fundamentais das pessoas singulares têm evoluído, no âmbito da constituição, por meio da jurisprudência, das referidas leis, e de tratados internacionais, em particular a Convenção Europeia dos Direitos Humanos (CEDH), que o Reino Unido ratificou em 1951. Em 1987, o Reino Unido também ratificou a Convenção do Conselho da Europa para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal (Convenção 108) ([10]).

(10) O *Human Rights Act 1998* incorpora os direitos constantes da Convenção Europeia dos Direitos Humanos no direito do Reino Unido. Concede a todas as pessoas os direitos e as liberdades fundamentais previstos nos artigos 2.º a 12.º e no artigo 14.º da Convenção Europeia dos Direitos Humanos, nos artigos 1.º, 2.º e 3.º 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.º e 18.º da referida convenção. Tal inclui o direito ao respeito pela vida privada e familiar (e o direito à proteção de dados no âmbito desse direito), bem como o direito a um processo equitativo ([11]). Concretamente, nos termos do artigo 8.º da referida convenção, só pode haver ingerência da autoridade pública no exercício do direito à privacidade, se tal ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, a segurança pública, o bem-estar económico do país, a defesa da ordem e a prevenção das infrações penais, a proteção da saúde ou da moral, ou a proteção dos direitos e das liberdades de terceiros.

(11) Em conformidade com o *Human Rights Act 1998*, qualquer ação das autoridades públicas deve ser compatível com um direito da convenção ([12]). Além disso, o direito primário e o direito derivado têm de ser interpretados e aplicados de uma forma que seja compatível com os direitos da convenção ([13]).

2.2. **Quadro do Reino Unido em matéria de proteção de dados**

(12) O Reino Unido saiu da União Europeia em 31 de janeiro de 2020. Ao abrigo do 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 ([14]), o direito da União continuou a aplicar-se no Reino Unido durante o período de transição até 31 de dezembro de 2020. Antes da saída e durante o período de transição, o quadro legislativo em matéria de proteção de dados pessoais no Reino Unido consistia na legislação aplicável da UE [nomeadamente o Regulamento (UE) 2016/679 e a Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho ([15])] e na legislação nacional, nomeadamente o *Data Protection Act 2018* (DPA 2018) ([16]), que previa regras nacionais, quando permitido pelo Regulamento (UE) 2016/679, que especificam e limitam a aplicação das regras do Regulamento (UE) 2016/679, e que transpôs a Diretiva (UE) 2016/680.

([10]) Os princípios da Convenção 108 foram inicialmente transpostos para o direito do Reino Unido através do *Data Protection Act* de 1984, que foi substituído pelo DPA 1998, o qual, por sua vez, foi substituído pelo DPA 2018 (lido em conjugação com o RGPD do Reino Unido). Em 2018, o Reino Unido assinou igualmente o Protocolo que altera a Convenção para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal (designado por «Convenção 108+») e encontra-se atualmente em processo de ratificação da convenção.

([11]) Artigos 6.º e 8.º da CEDH (ver também o *schedule 1* do *Human Rights Act 1998*).

([12]) *Section 6* do *Human Rights Act 1998*.

([13]) *Section 3* do *Human Rights Act 1998*.

([14]) 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 2019/C 384 I/01, XT/21054/2019/INIT (JO C 384 I de 12.11.2019, p. 1), disponível na seguinte ligação: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:12019W/TXT(02)&from=EN

([15]) 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), disponível na seguinte ligação: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016L0680&from=EN

([16]) *Data Protection Act 2018*, disponível na seguinte ligação: https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

(13) Para preparar a saída da União Europeia, o Governo do Reino Unido promulgou o *European Union (Withdrawal) Act 2018* [Lei de 2018 sobre a (Saída da) União Europeia] ([17]), que incorpora legislação da União diretamente aplicável no direito do Reino Unido ([18]). O denominado «direito da UE mantido» inclui o Regulamento (UE) 2016/679 na sua totalidade (incluindo os seus considerandos) ([19]). Nos termos da referida lei, o direito da UE mantido e inalterado tem de ser interpretado pelos tribunais do Reino Unido em conformidade com a jurisprudência aplicável do Tribunal de Justiça Europeu e com os princípios gerais do direito da União, pois produzem efeitos imediatamente antes do termo do período de transição (denominados, respetivamente, «jurisprudência da UE mantida» e «princípios gerais do direito da UE mantidos») ([20]).

(14) Ao abrigo do *European Union (Withdrawal) Act 2018*, os ministros do Reino Unido têm o poder de introduzir atos do direito derivado, através de instrumentos estatutários, a fim de efetuar as alterações necessárias ao direito da União Europeia mantido em consequência da saída do Reino Unido da União Europeia. Exerceram esse poder ao adotar os *Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019* [Regulamentos de 2019 relativos à Proteção de Dados, à Privacidade e às Comunicações Eletrónicas (alterações, etc.) (saída da UE) – Regulamentos DPPEC] ([21]). Os Regulamentos DPPEC alteram o Regulamento (UE) 2016/679, conforme introduzido no direito britânico através do *European Union (Withdrawal) Act 2018*, o DPA 2018 e outra legislação em matéria de proteção de dados para os adequarem ao contexto nacional ([22]).

(15) Por conseguinte, o quadro jurídico em matéria de proteção de dados pessoais no Reino Unido, após o termo do período de transição, consiste:

— no RGPD do Reino Unido, conforme incorporado no direito do Reino Unido ao abrigo do *European Union (Withdrawal) Act 2018* e alterado pelos Regulamentos DPPEC ([23]), e

— no DPA 2018 ([24]), com a redação que lhe foi dada pelos Regulamentos DPPEC.

(16) Como o RGPD do Reino Unido é baseado na legislação da UE, em muitos aspetos, as regras relativas à proteção de dados no Reino Unido refletem fielmente as regras correspondentes aplicáveis na União Europeia.

(17) Além dos poderes conferidos ao ministro da tutela pelo *European Union (Withdrawal) Act 2018*, várias disposições do DPA 2018 conferem-lhe poderes para adotar atos de direito derivado para alterar determinadas disposições da lei ou prever regras complementares ou adicionais ([25]). Até ao momento, o ministro da tutela só exerceu o poder ao abrigo

([17]) *European Union (Withdrawal) Act 2018*, disponível na seguinte ligação: https://www.legislation.gov.uk/ukpga/2018/16/contents

([18]) A intenção e o efeito do *European Union (Withdrawal) Act 2018* é que toda a legislação direta da União que tenha sido incorporada no direito do Reino Unido no final do período de transição seja incorporada no direito do Reino Unido, uma vez que produz efeitos no direito da UE imediatamente antes do final do período de transição. Ver *section 3* do *European Union (Withdrawal) Act 2018*.

([19]) As *Explanatory Notes* (notas explicativas) do *European Union Withdrawal Act 2018* especificam o seguinte: «Sempre que a legislação seja convertida ao abrigo da presente secção, é o texto da própria legislação que fará parte da legislação nacional. Tal incluirá o texto integral de qualquer instrumento da UE (nomeadamente os seus considerandos).». [*Explanatory Notes* do *European Union Withdrawal Act 2018*, n.º 83, disponível na seguinte ligação: https://www.legislation.gov.uk/ukpga/2018/16/pdfs/ukpgaen_20180016_en.pdf]. De acordo com as informações fornecidas pelas autoridades do Reino Unido, como os considerandos não têm o estatuto de normas jurídicas vinculativas, não foi necessário alterá-los da mesma forma que os artigos do Regulamento (UE) 2016/679 foram alterados pelos Regulamentos DPPEC.

([20]) *Section 6* do *European Union (Withdrawal) Act 2018*.

([21]) *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 lhes foi dada pelos Regulamentos DPPEC de 2020, disponíveis na seguinte ligação: https://www.legislation.gov.uk/ukdsi/2020/9780348213522

([22]) Estas alterações do RGPD do Reino Unido e do DPA 2018 são principalmente de natureza técnica, como a supressão de referências a «Estados-Membros» ou o ajustamento da terminologia, por exemplo, a substituição de referências ao Regulamento (UE) 2016/679 por referências ao RGPD do Reino Unido. Em alguns casos, foram necessárias alterações para refletir o contexto puramente nacional das disposições, por exemplo, no que respeita a «quem» adota «regulamentos de adequação» para efeitos do quadro jurídico em matéria de proteção de dados do Reino Unido (ver *section 17A* do DPA 2018), ou seja, o ministro da tutela (*Secretary of State*) em vez da Comissão Europeia.

([23]) *General Data Protection Regulation, Keeling Schedule*, disponível na seguinte ligação: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/946117/20201102_-_GDPR_-__MASTER__Keeling_Schedule__with_changes_highlighted__V3.pdf

([24]) *Data Protection Act 2018, Keeling Schedule*, disponível na seguinte ligação: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/946100/20201102_-_DPA_-__MASTER__Keeling_Schedule__with_changes_highlighted__V3.pdf

([25]) Tais poderes constam, por exemplo, da *section 16* (poder para fazer, em situações específicas, estritamente circunscritas, outras isenções a disposições específicas do RGPD do Reino Unido), *section 17A* (poder para adotar regulamentos de adequação), *sections 212* e *213* (poderes para iniciar legislação e fazer disposições transitórias), e *section 211* (poder para fazer alterações menores e consequentes) do DPA 2018.

da *section 137* do DPA 2018 para adotar os *Data Protection (Charges and Information) (Amendment) Regulations 2019* [Regulamentos de 2019 relativos à Proteção de Dados (taxas e informações) (alteração)], que estabelecem as circunstâncias em que os responsáveis pelo tratamento são obrigados a pagar uma taxa anual ao comissário para a informação (*Information Commissioner*), a autoridade independente de proteção de dados do Reino Unido.

(18) Por último, são fornecidas mais orientações sobre a legislação do Reino Unido em matéria de proteção de dados nos códigos de boas práticas e noutras orientações adotadas pelo comissário para a informação. Embora não sejam formalmente vinculativas, tais orientações têm um peso interpretativo e demonstram a forma como a legislação em matéria de proteção de dados é aplicada e executada, na prática, pelo comissário. Em particular, as *sections 121* a *125* do DPA 2018 exigem que o comissário elabore códigos de boas práticas sobre a partilha de dados, a comercialização direta, a elaboração adequada à idade e a proteção de dados e o jornalismo.

(19) Na sua estrutura e principais componentes, o quadro jurídico do Reino Unido aplicável aos dados transferidos ao abrigo da presente decisão é, por conseguinte, muito semelhante ao que se aplica na União Europeia. Tal inclui o facto de não se basear apenas nas obrigações estabelecidas no direito interno, que foram influenciadas pelo direito da UE, mas também em obrigações consagradas no direito internacional, em particular através da adesão do Reino Unido à CEDH e à Convenção 108, bem como na sua submissão à competência jurisdicional do Tribunal Europeu dos Direitos Humanos. Estas obrigações decorrentes de instrumentos internacionais juridicamente vinculativos, relativos, nomeadamente, à proteção de dados pessoais, constituem, por conseguinte, um elemento particularmente importante do quadro jurídico avaliado na presente decisão.

2.3. **Âmbito de aplicação material e territorial**

(20) À semelhança do Regulamento (UE) 2016/679, o RGPD do Reino Unido aplica-se ao tratamento de dados pessoais por meios total ou parcialmente automatizados, ou a outro tratamento, se os dados pessoais estiverem contidos num ficheiro ([26]). As definições de «dados pessoais», de «titular dos dados» e de «tratamento» do RGPD do Reino Unido são idênticas às do Regulamento (UE) 2016/679 ([27]). Além disso, o RGPD do Reino Unido aplica-se ao tratamento de dados pessoais manuais não estruturados ([28]) detidos por determinadas autoridades públicas do Reino Unido ([29]), embora a aplicação dos princípios e direitos do RGPD do Reino Unido que não sejam pertinentes para esses dados pessoais seja afastada pelas *sections 24* e *25* do DPA 2018. À semelhança do previsto no Regulamento (UE) 2016/679, o RGPD do Reino Unido não se aplica ao tratamento de dados pessoais efetuado por pessoas singulares no exercício de atividades exclusivamente pessoais ou domésticas ([30]).

(21) O RGPD do Reino Unido amplia o seu âmbito de aplicação também ao tratamento no exercício de atividades que, imediatamente antes do termo do período de transição, se encontravam fora do âmbito de aplicação do direito da União Europeia (como a segurança nacional) ([31]), ou que estavam abrangidas pelo âmbito de aplicação do título V, capítulo 2, do Tratado da União Europeia (atividades da política externa e de segurança comum) ([32]). Tal como no sistema da União Europeia, o RGPD do Reino Unido não se aplica ao tratamento de dados pessoais por uma autoridade competente para efeitos de prevenção, investigação, deteção e repressão de infrações penais ou da

([26]) Artigo 2.º, n.ºs 1 e 5, do RGPD do Reino Unido.

([27]) Artigo 4.º, n.ºs 1 e 2, do RGPD do Reino Unido.

([28]) O tratamento manual não estruturado de dados pessoais é definido no artigo 2.º, n.º 5, alínea b), como o tratamento de dados pessoais que não o tratamento automatizado ou estruturado de dados pessoais.

([29]) O artigo 2.º, n.º 1A, do RGPD do Reino Unido prevê que o regulamento também se aplica ao tratamento manual não estruturado de dados pessoais detidos por uma autoridade pública FOI. A referência a autoridades públicas FOI significa qualquer autoridade pública tal como definida no *Freedom of Information Act 2000* (Lei de 2000 relativa à Liberdade de Informação), ou qualquer autoridade pública escocesa conforme definida no *Freedom of Information (Scotland) Act 2002 (asp 13)* [Lei de 2002 relativa à Liberdade de Informação (Escócia) (*asp 13*)]. *Section 21(5)* do DPA 2018.

([30]) Artigo 2.º, n.º 2, alínea a), do RGPD do Reino Unido.

([31]) As atividades de segurança nacional só são abrangidas pelo âmbito de aplicação do RGPD do Reino Unido se não forem efetuadas por uma autoridade competente para efeitos de aplicação da lei, caso em que se aplica a parte 3 do DPA 2018, ou por ou em nome de um serviço de informações, cujas atividades estejam excluídas do âmbito de aplicação do RGPD do Reino Unido e sujeitas à parte 4 do DPA 2018 nos termos do artigo 2.º, n.º 2, alínea c), do RGPD do Reino Unido. Por exemplo, uma força policial pode efetuar controlos de segurança relativamente a um funcionário para garantir que se pode confiar nele para ter acesso a material de segurança nacional. Apesar de a polícia ser uma autoridade competente para efeitos de aplicação da lei, o tratamento em questão não se destina a esses feitos e o RGPD do Reino Unido seria aplicável. Ver *Explanatory Framework for Adequacy Discussions, section H: National Security Data Protection and Investigatory Powers Framework* (Enquadramento explicativo do Reino Unido para discussões de adequação, secção H: quadro da proteção de dados para fins de segurança nacional e dos poderes de investigação), p. 8, disponível na seguinte ligação: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872239/H_-_National_Security.pdf

([32]) Artigo 2.º, n.º 1, alíneas a) e b), do RGPD do Reino Unido.

execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública (os chamados «efeitos de aplicação da lei») — tal tratamento é regido pela parte 3 do DPA 2018, como é o caso da Diretiva (UE) 2016/680 ao abrigo do direito da União Europeia — ou ao tratamento de dados pessoais pelos serviços de informações [o *Security Service* (serviço de segurança), o *Secret Intelligence Service* (serviço de informações secretas) e o *Government Communications Headquarter* (quartel-general de comunicações do Estado)], que é abrangido pela parte 4 do DPA 2018 ([33]).

(22) O âmbito de aplicação territorial do RGPD do Reino Unido é descrito no artigo 3.º do RGPD do Reino Unido ([34]) e inclui o tratamento de dados pessoais (independentemente do local onde ocorra) no contexto das atividades de um estabelecimento de um responsável pelo tratamento ou de um subcontratante no Reino Unido, bem como o tratamento de dados pessoais de titulares que se encontrem no Reino Unido, quando as atividades de tratamento estejam relacionadas com a oferta de bens ou serviços a esses titulares de dados ou com o controlo do seu comportamento ([35]). Tal reflete a abordagem adotada no artigo 3.º do Regulamento (UE) 2016/679.

2.4. **Definições de dados pessoais e conceitos de responsável pelo tratamento e subcontratante**

(23) As definições de dados pessoais, tratamento, responsável pelo tratamento, subcontratante, bem como de pseudonimização, estabelecidas no Regulamento (UE) 2016/679, foram mantidas sem alterações significativas no RGPD do Reino Unido ([36]). Além disso, o artigo 9.º, n.º 1, do RGPD do Reino Unido define as categorias especiais de dados da mesma forma que o Regulamento (UE) 2016/679 («dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa»). A *section 205* do DPA 2018 fornece a definição de «dados biométricos» ([37]), «dados relativos à saúde» ([38]) e «dados genéticos» ([39]).

2.5. **Garantias, direitos e obrigações**

2.5.1. *Licitude e lealdade do tratamento*

(24) Os dados pessoais devem ser objeto de um tratamento lícito e leal.

(25) Os princípios da licitude, lealdade e transparência, bem como os fundamentos para o tratamento lícito são garantidos no direito do Reino Unido através do artigo 5.º, n.º 1, alínea a), e do artigo 6.º, n.º 1, do RGPD do Reino Unido, que são idênticos às respetivas disposições do Regulamento (UE) 2016/679 ([40]). A *section 8* do DPA 2018

([33]) Artigo 2.º, n.º 2, alíneas b) e c), do RGPD do Reino Unido.

([34]) O mesmo âmbito de aplicação territorial aplica-se ao tratamento de dados pessoais ao abrigo da parte 2 do DPA 2018, que complementa o RGPD do Reino Unido [*section 207(1A)*].

([35]) Tal significa, nomeadamente, que o DPA de 2018 e, por conseguinte, a presente decisão não são aplicáveis às dependências da Coroa do Reino Unido (Jersey, Guernesey e a Ilha de Man) e aos territórios ultramarinos do Reino Unido, como, por exemplo, as Ilhas Falkland e o território de Gibraltar.

([36]) Artigo 4.º, n.ºs 1, 2, 5, 7 e 8, do RGPD do Reino Unido.

([37]) «Dados biométricos», dados pessoais resultantes de um tratamento técnico específico relativo às características físicas, fisiológicas ou comportamentais de uma pessoa singular que permitam ou confirmem a identificação única dessa pessoa singular, nomeadamente imagens faciais ou dados dactiloscópicos.

([38]) «Dados relativos à saúde», dados pessoais relativos à saúde física ou mental de uma pessoa singular, incluindo a prestação de serviços de saúde, que revelem informações sobre o seu estado de saúde.

([39]) «Dados genéticos», os dados pessoais relativos às características genéticas, hereditárias ou adquiridas, de uma pessoa singular que deem informações únicas sobre a fisiologia ou a saúde dessa pessoa singular e que resultem designadamente de uma análise de uma amostra biológica proveniente da pessoa singular em causa.

([40]) Nos termos do artigo 6.º, n.º 1 do RGPD do Reino Unido, o tratamento só é lícito se e na medida em que: a) o titular dos dados tiver dado o seu consentimento para o tratamento dos seus dados pessoais para uma ou mais finalidades específicas; b) o tratamento for necessário para a execução de um contrato no qual o titular dos dados é parte, ou para diligências pré-contratuais a pedido do titular dos dados; c) o tratamento for necessário para o cumprimento de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito; d) o tratamento for necessário para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular; e) o tratamento for necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento; ou f) o tratamento for necessário para efeito dos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros, exceto se prevalecerem os interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, em especial se o titular for uma criança.

complementa o artigo 6.º, n.º 1, alínea e), ao prever que o tratamento de dados pessoais ao abrigo do artigo 6.º, n.º 1, alínea e), do RGPD do Reino Unido (necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública do responsável pelo tratamento), inclui o tratamento de dados pessoais que seja necessário à administração da justiça, ao exercício de uma função das câmaras do parlamento, ao exercício de uma função conferida a uma pessoa por uma texto legislativo ou pelo Estado de direito, ao exercício de uma função da Coroa, de um ministro da Coroa ou de um departamento governamental, ou a uma atividade que apoie ou promova a participação democrática.

(26) No que respeita ao consentimento (um dos fundamentos para o tratamento lícito), o RGPD do Reino Unido também mantém inalteradas as condições previstas no artigo 7.º do Regulamento (UE) 2016/679, ou seja, o responsável pelo tratamento deve poder demonstrar que o titular dos dados deu o seu consentimento, deve ser apresentado um pedido de consentimento escrito numa linguagem clara e simples, o titular dos dados deve ter o direito de retirar o consentimento a qualquer momento, e ao avaliar se o consentimento é dado livremente, deve ter-se em conta se a execução de um contrato está subordinada ao consentimento para o tratamento de dados pessoais que não seja necessário para a execução desse contrato. Além disso, nos termos do artigo 8.º do RGPD do Reino Unido, no contexto da prestação de serviços da sociedade da informação, o consentimento de uma criança só é lícito se esta tiver, pelo menos, 13 anos. Tal enquadra-se na faixa etária estabelecida no artigo 8.º do Regulamento (UE) 2016/679.

2.5.2. *Tratamento de categorias especiais de dados pessoais*

(27) Devem existir garantias específicas aplicáveis ao tratamento de «categorias especiais» de dados.

(28) O RGPD do Reino Unido e o DPA 2018 contêm regras específicas no que respeita ao tratamento de categorias especiais de dados pessoais, que são definidas no artigo 9.º, n.º 1, do RGPD do Reino Unido da mesma forma que no Regulamento (UE) 2016/679 (ver considerando 23). Nos termos do artigo 9.º do RGPD do Reino Unido, o tratamento de categorias especiais de dados é, em princípio, proibido, a menos que se aplique uma exceção específica.

(29) Tais exceções (indicadas no artigo 9.º, n.ºs 2 e 3, do RGPD do Reino Unido) não introduzem quaisquer alterações de fundo às constantes do artigo 9.º, n.ºs 2 e 3, do Regulamento (UE) 2016/679. A menos que o titular dos dados tenha dado o seu consentimento explícito para o tratamento desses dados pessoais, o tratamento de categorias especiais de dados pessoais só é permitido em circunstâncias específicas e limitadas. Na maioria dos casos, o tratamento de dados sensíveis tem de ser necessário para uma finalidade específica, definida na disposição aplicável [ver o artigo 9.º, n.º 2, alíneas b), c), f), g), h), i) e j)].

(30) Além disso, quando uma exceção ao abrigo do artigo 9.º, n.º 2, do RGPD do Reino Unido exige uma autorização por lei ou refere o interesse público, a *section 10* do DPA 2018, em conjunto com o *schedule 1* do DPA 2018 especificam ainda as condições que devem ser cumpridas para que as exceções possam ser invocadas. Por exemplo, no caso do tratamento de dados sensíveis para proteger a «saúde pública» [artigo 9.º, n.º 2, alínea i), do RGPD do Reino Unido], o *schedule 1*, parte 1, n.º 3, alínea b), exige que, além do critério da necessidade, tal tratamento seja efetuado «por ou sob a responsabilidade de um profissional de saúde» ou «por outra pessoa que tenha um dever de confidencialidade ao abrigo de um texto legislativo ou do Estado de direito», incluindo ao abrigo do dever consagrado de confidencialidade do direito comum.

(31) Em caso de tratamento de dados sensíveis por motivos de interesse público importante [artigo 9.º, n.º 2, alínea g), do RGPD do Reino Unido], o *schedule 1*, parte 2, do DPA 2018 prevê uma lista exaustiva de finalidades que podem ser consideradas de interesse público importante, estabelecendo, para cada um delas, condições adicionais específicas. Por exemplo, a promoção da diversidade racial e étnica nos níveis superiores das organizações é reconhecida como um interesse público importante. O tratamento de dados sensíveis para esta finalidade específica está sujeito a requisitos pormenorizados, nomeadamente que o tratamento seja efetuado como parte de um processo de identificação de pessoas adequadas para ocupar cargos superiores, seja necessário para promover a diversidade racial e étnica, e não seja suscetível de causar danos substanciais ou sofrimento emocional substancial ao titular dos dados.

(32) A *section 11(1)* do DPA 2018 estabelece as condições para o tratamento de dados pessoais nas circunstâncias descritas no artigo 9.º, n.º 3, do RGPD do Reino Unido, relacionadas com a obrigação de confidencialidade. Tal inclui circunstâncias em que o tratamento é efetuado por ou sob a responsabilidade de um profissional de saúde ou de um assistente social, ou por outra pessoa que, nessas circunstâncias, tenha um dever de confidencialidade ao abrigo de um texto legislativo ou do Estado de direito.

(33) Além disso, muitas das exceções indicadas no artigo 9.º, n.º 2, do RGPD do Reino Unido exigem garantias adequadas e específicas para poderem ser utilizadas. Em função da natureza do tratamento e do nível de risco para os direitos e as liberdades dos titulares dos dados, as condições para o tratamento previstas no *schedule 1* do DPA 2018 estabelecem garantias diferentes. O *schedule 1* estabelece, sucessivamente, as condições para cada situação de tratamento.

(34) Em alguns casos, o DPA 2018 regula e limita o tipo de dados sensíveis que podem ser tratados para que uma determinada base jurídica seja cumprida. Por exemplo, o *schedule 1*, n.º 8, autoriza o tratamento de dados sensíveis para efeitos da promoção da igualdade de oportunidades ou de tratamento. Esta condição de tratamento só pode ser utilizada se os dados revelarem origem racial ou étnica, convicções religiosas ou filosóficas, orientação sexual, ou se se tratar de dados relativos à saúde.

(35) Em alguns casos, o DPA 2018 limita o tipo de responsável pelo tratamento que pode utilizar a condição de tratamento. Por exemplo, o *schedule 1*, n.º 23, prevê o tratamento de dados sensíveis relativos às respostas dos representantes eleitos ao público. Esta condição de tratamento só pode ser utilizada se o responsável pelo tratamento for o representante eleito ou estiver a agir sob a sua autoridade.

(36) Noutros outros casos, o DPA 2018 estabelece limites às categorias dos titulares dos dados que podem utilizar a condição de tratamento. Por exemplo, o *schedule 1*, n.º 21, regulamenta o tratamento de dados sensíveis para regimes profissionais de pensões. Esta condição só pode ser utilizada se o titular dos dados for irmão ou irmã, progenitor, avô ou avó, ou bisavô ou bisavó do inscrito.

(37) Além disso, ao invocar as exceções constantes do artigo 9.º, n.º 2, do RGPD do Reino Unido, que estão especificadas com mais pormenor na *section 10* do DPA 2018, em conjunto com o *schedule 1* do DPA 2018, na maioria dos casos, o responsável pelo tratamento é obrigado a elaborar um documento de políticas adequado (*appropriate policy document*). Tal documento deve explicar os procedimentos do responsável pelo tratamento para garantir a conformidade com os princípios do artigo 5.º do RGPD do Reino Unido. Deve também descrever as políticas para a conservação e o apagamento, com indicação do prazo provável de conservação. Os responsáveis pelo tratamento têm de rever e atualizar o documento, conforme adequado. O responsável pelo tratamento deve conservar o referido documento de políticas durante seis meses após a conclusão do tratamento e colocá-lo à disposição do comissário para a informação, a pedido ([41]).

(38) Nos termos do *schedule 1*, n.º 41, do DPA 2018, o documento de políticas deve ser sempre acompanhado por um registo alargado do tratamento, que deve conter o seguimento dos compromissos incluídos no documento de políticas, ou seja, se os dados estão a ser apagados ou retidos de acordo com as políticas. Se tal não se verificar, o registo tem de indicar as razões. Deve também descrever como o tratamento satisfaz o artigo 6.º do RGPD do Reino Unido (licitude do tratamento) e a condição específica do *schedule 1* do DPA 2018 em que se baseia.

(39) Por último, tal como o Regulamento (UE) 2016/679, o RGPD do Reino Unido também prevê garantias gerais para determinadas operações de tratamento de categorias especiais de dados. O artigo 35.º do RGPD do Reino Unido exige uma avaliação de impacto sobre a proteção de dados em caso de operações de tratamento em grande escala de categorias especiais de dados. Nos termos do artigo 37.º do RGPD do Reino Unido, um responsável pelo tratamento ou subcontratante tem de designar um encarregado da proteção de dados sempre que as suas atividades principais consistam em operações de tratamento em grande escala de categorias especiais de dados.

(40) No que respeita aos dados pessoais relacionados com condenações penais e infrações, o artigo 10.º do RGPD do Reino Unido é idêntico ao artigo 10.º do Regulamento (UE) 2016/679. Permite o tratamento de dados pessoais relacionados com condenações penais e infrações apenas sob o controlo de uma autoridade pública ou se o tratamento for autorizado por disposições do direito interno que prevejam garantias adequadas para os direitos e liberdades dos titulares dos dados.

(41) Quando o tratamento de dados relacionados com condenações penais e infrações não for efetuado sob o controlo de uma autoridade pública, a *section 10(5)* do DPA 2018 prevê que esse tratamento só possa ter lugar para as finalidades/nas situações específicas estabelecidas nas partes 1, 2 e 3 do *schedule 1* do DPA 2018 e esteja sujeito aos requisitos específicos estabelecidos para cada uma dessas finalidades/situações. Por exemplo, os dados pessoais relativos às condenações penais podem ser tratados por organismos sem fins lucrativos se o tratamento for efetuado a) no âmbito das suas atividades legítimas e mediante garantias adequadas, por uma fundação, associação ou qualquer outro organismo sem fins lucrativos e que prossiga fins políticos, filosóficos, religiosos ou sindicais, e b) desde que i) esse tratamento se refira exclusivamente aos membros ou antigos membros desse organismo ou a pessoas que com ele tenham mantido contactos regulares relacionados com os seus objetivos, e ii) que os dados pessoais não sejam divulgados a terceiros sem o consentimento dos seus titulares.

([41]) *Schedule 1*, n.ºs 38-40, do DPA 2018.

(42) Além disso, a parte 3 do *schedule 1* do DPA 2018 prevê outras circunstâncias em que os dados pessoais relativos às condenações penais podem ser utilizados, que correspondem aos fundamentos jurídicos para o tratamento de dados sensíveis constantes do artigo 9.º, n.º 2, do Regulamento (UE) 2016/679 e do RGPD do Reino Unido (por exemplo, o consentimento do titular dos dados, os interesses vitais de uma pessoa singular se o titular dos dados estiver física ou legalmente incapacitado de dar o seu consentimento, se os dados pessoais já tiverem sido manifestamente tornados públicos pelo seu titular, se o tratamento for necessário à declaração, ao exercício ou à defesa de um direito num processo judicial, etc.).

2.5.3 *Limitação das finalidades, exatidão, minimização dos dados, limitação da conservação e segurança dos dados*

(43) Os dados pessoais 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.

(44) Este princípio está previsto no artigo 5.º, n.º 1, alínea b), do Regulamento (UE) 2016/679 e foi mantido, sem alterações, no artigo 5.º, n.º 1, alínea b), do RGPD do Reino Unido. As condições relativas ao tratamento posterior compatível nos termos do artigo 6.º, n.º 4, do Regulamento (UE) 2016/679 também foram mantidas sem alterações significativas no artigo 6.º, n.º 4, alíneas a) a e), do RGPD do Reino Unido.

(45) Além disso, os dados devem ser exatos e, quando necessário, objeto de atualização. Devem também ser adequados, pertinentes e não excessivos relativamente às finalidades para que são tratados e, em princípio, não devem ser conservados por mais tempo do que o necessário para as finalidades para que são tratados.

(46) Estes princípios de minimização dos dados, exatidão e limitação da conservação estão estabelecidos no artigo 5.º, n.º 1, alíneas c) a e), do Regulamento (UE) 2016/679 e foram mantidos sem alterações no artigo 5.º, n.º 1, alíneas c) a e), do RGPD do Reino Unido.

(47) Os dados pessoais também devem ser tratados de uma forma que garanta a sua segurança, incluindo proteção contra tratamento não autorizado ou ilícito e contra perda, destruição ou danos acidentais. Para este fim, os operadores comerciais devem tomar as medidas técnicas e organizativas adequadas para proteger os dados pessoais contra eventuais ameaças. Estas medidas devem ser avaliadas, tendo em consideração o estado atual dos conhecimentos e os custos conexos.

(48) A segurança dos dados está consagrada no direito do Reino Unido por meio do princípio de integridade e confidencialidade constante do artigo 5.º, n.º 1, alínea f), do RGPD do Reino Unido, bem como do seu artigo 32.º sobre a segurança do tratamento. Essas disposições são idênticas às respetivas disposições do Regulamento (UE) 2016/679. Além disso, nas mesmas condições que as estabelecidas nos artigos 33.º e 34.º do Regulamento (UE) 2016/679, o RGPD do Reino Unido exige a notificação de uma violação de dados pessoais à autoridade de controlo (artigo 33.º do RGPD do Reino Unido) e a comunicação de uma violação de dados pessoais ao titular dos dados (artigo 34.º do RGPD do Reino Unido).

2.5.4 *Transparência*

(49) Os titulares dos dados devem ser informados sobre as principais características do tratamento dos respetivos dados pessoais.

(50) Tal é assegurado pelos artigos 13.º e 14.º do RGPD do Reino Unido que, além de um princípio geral de transparência, preveem regras sobre as informações a facultar ao titular dos dados ([42]). O RGPD do Reino Unido não introduz alterações significativas a estas regras em comparação com os artigos correspondentes do Regulamento (UE) 2016/679. No entanto, como no Regulamento (UE) 2016/679, os requisitos de transparência desses artigos estão sujeitos a várias exceções previstas no DPA 2018 (ver considerandos 55 a 72).

([42]) No artigo 13.º, n.º 1, alínea f), e no artigo 14.º, n.º 1, alínea f), as referências a decisões de adequação adotadas pela Comissão foram substituídas por referências a instrumentos equivalentes do Reino Unido, ou seja, regulamentos de adequação ao abrigo do DPA 2018. Além disso, no artigo 14.º, n.º 5, alíneas c) e d), as referências ao direito da UE ou do Estado-Membro foram substituídas por uma referência ao direito interno [como exemplos do direito interno que podem estar abrangidos pelo artigo 14.º, n.º 5, alínea c), o Reino Unido referiu a *section 7* do *Scrap Metal Dealers Act 2013* (Lei de 2013 relativa aos Comerciantes de Sucata Metálica), que prevê regras para o registo das licenças de sucata metálica, ou a parte 35 do *Companies Act 2006* (Lei das Sociedades de 2006), que prevê as regras para o registo das sociedades. Da mesma forma, um exemplo de direito interno que poderá ser abrangido pelo artigo 14.º, n.º 5, alínea d), pode incluir legislação que estabeleça regras em matéria de confidencialidade profissional, ou obrigações refletidas nos contratos de trabalho ou o dever de confidencialidade do direito comum (como dados pessoais tratados por profissionais de saúde, recursos humanos, assistentes sociais, etc.)].

2.5.5 *Direitos individuais*

(51) Os titulares dos dados devem ter determinados direitos que podem ser exercidos contra o responsável pelo tratamento ou subcontratante, nomeadamente o direito de acesso aos dados, o direito de oposição ao tratamento, e o direito de retificação e apagamento dos dados. Ao mesmo tempo, tais direitos podem estar sujeitos a limitações, na medida em que estas sejam necessárias e proporcionadas para assegurar a segurança pública ou outros objetivos importantes do interesse público geral.

2.5.5.1 Direitos materiais

(52) O RGPD do Reino Unido confere às pessoas singulares os mesmos direitos oponíveis que o Regulamento (UE) 2016/679. As disposições que preveem os direitos das pessoas singulares foram mantidas no RGPD do Reino Unido sem alterações significativas.

(53) Os direitos incluem o direito de acesso do titular dos dados (artigo 15.º do RGPD do Reino Unido), o direito de retificação (artigo 16.º do RGPD do Reino Unido), o direito ao apagamento dos dados (artigo 17.º do RGPD do Reino Unido), o direito à limitação do tratamento (artigo 18.º do RGPD do Reino Unido), uma obrigação de notificação da retificação ou apagamento dos dados pessoais ou limitação do tratamento (artigo 19.º do RGPD do Reino Unido), o direito de portabilidade dos dados (artigo 20.º do RGPD do Reino Unido), e o direito de oposição (artigo 21.º do RGPD do Reino Unido) ([43]). Este último inclui também o direito do titular dos dados de se opor ao tratamento de dados pessoais para efeitos de comercialização direta previsto no artigo 21.º, n.ºs 2 e 3, do Regulamento (UE) 2016/679. Além disso, nos termos da *section 122* do DPA 2018, o comissário para a informação deve elaborar um código de boas práticas relativamente à realização da comercialização direta, de acordo com os requisitos da legislação em matéria de proteção de dados [e dos *Privacy and Electronic Communications (EC Directive) Regulations 2003* (Regulamentos de 2003 relativos à Privacidade e às Comunicações Eletrónicas (Diretiva CE))] e outras orientações para promover as boas práticas na comercialização direta que considere adequadas. O Gabinete do Comissário para a Informação (*Information Commissioner's Office*, ICO) está atualmente a elaborar um código relativo à comercialização direta ([44]).

(54) O direito do titular dos dados de não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado, que produza efeitos na sua esfera jurídica ou que o afete significativamente de forma similar, conforme previsto no artigo 22.º do RGPD, também foi mantido no RGPD do Reino Unido sem alterações significativas. No entanto, foi aditado um novo n.º 3-A para referir que a *section 14* do DPA 2018 estabelece garantias para salvaguardar os direitos, as liberdades e os interesses legítimos dos titulares dos dados quando o tratamento é efetuado ao abrigo do artigo 22.º, n.º 2, alínea b), do RGPD do Reino Unido, o que apenas se aplica quando a base para tal decisão é uma autorização ou requisito ao abrigo do direito do Reino Unido, não se aplicando quando a decisão é necessária nos termos de um contrato ou tomada com o consentimento explícito do titular dos dados. Quando se aplica a *section 14* do DPA 2018, o responsável pelo tratamento, assim que razoavelmente exequível, tem de notificar o titular dos dados por escrito de que foi tomada uma decisão exclusivamente com base no tratamento automatizado. No prazo de um mês após receber a notificação, o titular dos dados tem o direito de solicitar que o responsável pelo tratamento reconsidere a decisão ou tome uma nova que não se baseie exclusivamente no tratamento automatizado. O ministro da tutela está habilitado a adotar garantias adicionais no que respeita à tomada de decisões automatizada. Este poder ainda não foi exercido.

2.5.5.2 Limitações aos direitos individuais e outras disposições

(55) O DPA 2018 estabelece várias limitações aos direitos individuais, que se enquadram no âmbito do artigo 23.º do RGPD do Reino Unido. Não foram introduzidas quaisquer limitações neste quadro relativamente ao direito de oposição à comercialização direta, conforme previsto no artigo 21.º, n.ºs 2 e 3, do RGPD do Reino Unido, nem ao direito de não ficar sujeito a uma decisão automatizada, conforme previsto no artigo 22.º do RGPD do Reino Unido.

(56) As limitações estão pormenorizadas nos *schedules 2* a *4* do DPA 2018. As autoridades do Reino Unido explicaram que seguem dois princípios: o princípio da especificidade (adotando uma abordagem granular, dividindo limitações amplas em disposições múltiplas e mais específicas) e o princípio da condicionalidade (cada disposição é complementada por garantias sob a forma de limitações ou condições para evitar abusos) ([45]).

([43]) No artigo 17.º, n.º 1, alínea e), e no artigo 17.º, n.º 3, alínea b), as referências ao direito da UE ou de um Estado-Membro foram substituídas por uma referência ao direito interno [como exemplos do direito interno ao abrigo do artigo 17.º, n.º 1, alínea e), o Reino Unido referiu os *Education (Pupil Information) (England) Regulations 2006* (Regulamentos de 2006 relativos à Educação (informações dos alunos) (Inglaterra), que exigem que os nomes dos alunos sejam apagados dos registos escolares depois de terem deixado a escola, ou o *Medical Act 1983* (Lei Médica de 1983), *section 34F*, que estabelece as regras para a remoção de nomes do *General Practitioner Register* (Registo de Médicos de Clínica Geral) e do *Specialist Register* (Registo de Especialistas)].

([44]) O projeto de código de boas práticas pode ser encontrado na seguinte ligação: https://ico.org.uk/media/about-the-ico/consultations/2616882/direct-marketing-code-draft-guidance.pdf

([45]) *Explanatory Framework for Adequacy Discussions, Section E: Restrictions* (Enquadramento explicativo do Reino Unido para discussões de adequação, secção E: limitações), p. 1, disponível na seguinte ligação: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872232/E_-_Narrative_on_Restrictions.pdf

(57) As limitações descritas no artigo 23.º, n.º 1, do RGPD do Reino Unido foram concebidas por forma a garantir que apenas se aplicam em circunstâncias específicas, quando constituam uma medida necessária numa sociedade democrática e proporcionada ao objetivo legítimo visado. Além disso, em conformidade com a jurisprudência constante sobre a interpretação das limitações, uma isenção ao regime de proteção de dados só pode ser aplicada em qualquer caso particular se for necessário e proporcional fazê-lo ([46]). O critério da necessidade foi exigido como «um critério rigoroso, que exige que qualquer ingerência nos direitos do titular dos dados seja proporcional à gravidade da ameaça ao interesse público. Por conseguinte, o exercício envolve uma análise clássica da proporcionalidade ([47])».

(58) O objetivo visado por estas limitações corresponde aos referidos no artigo 23.º do Regulamento (UE) 2016/679, com exceção das limitações relativas à segurança do Estado e à defesa, que são regulamentadas pela *section 26* do DPA 2018, mas que estão sujeitas aos mesmos requisitos de necessidade e proporcionalidade (ver considerandos 63 a 66).

(59) Algumas limitações, por exemplo, as relacionadas com a prevenção ou deteção da criminalidade, com a detenção ou repressão dos infratores, e com a liquidação ou cobrança de impostos ou taxas ([48]) permitem limitações a todos os direitos individuais e obrigações de transparência (excluindo os direitos nos termos do artigo 21.º, n.º 2, e do artigo 22.º). O alcance de outras limitações está limitado às obrigações de transparência e aos direitos de acesso, como as limitações relativas à confidencialidade das comunicações entre advogados e clientes ([49]), ao direito de não cumprir o requisito de fornecer informações suscetíveis de levar à autoincriminação ([50]), e ao financiamento das empresas, nomeadamente a prevenção do abuso de informação privilegiada ([51]). Poucas limitações permitem uma limitação à obrigação do responsável pelo tratamento de comunicar uma violação de dados a um titular dos dados e aos princípios da limitação das finalidades e da licitude, lealdade e transparência do tratamento ([52]).

(60) Algumas limitações aplicam-se automaticamente «na íntegra» a um determinado tipo de tratamento de dados pessoais (por exemplo, a aplicação das obrigações de transparência e dos direitos individuais é excluída quando os dados pessoais são tratados para efeitos de avaliação da adequação de uma pessoa para o exercício de funções jurisdicionais ou quando os dados pessoais são tratados por um tribunal ou pessoa singular, no exercício de uma competência judicial).

(61) No entanto, na maioria dos casos, o número pertinente do *schedule 2* do DPA 2018 especifica que a limitação só se aplica quando (e na medida em que) a aplicação das disposições «seria suscetível de prejudicar» o objetivo legítimo visado por essa limitação: por exemplo, as disposições referidas no RGPD do Reino Unido não se aplicam aos dados pessoais tratados para a prevenção ou deteção da criminalidade, para a detenção ou repressão dos infratores, ou para a liquidação ou cobrança de um imposto ou taxa «na medida em que a aplicação dessas disposições seria suscetível de prejudicar» qualquer uma dessas questões ([53]).

(62) O conceito «seria suscetível de prejudicar» tem sido interpretado repetidamente pelos tribunais do Reino Unido como «uma probabilidade muito significativa e importante de prejudicar os interesses públicos identificados» ([54]). Uma limitação sujeita ao critério do prejuízo só pode, por conseguinte, ser invocada se e na medida em que exista uma probabilidade muito significativa e importante de que a concessão de um determinado direito prejudicaria o interesse público em causa. O responsável pelo tratamento é responsável por avaliar numa base casuística se estas condições são cumpridas ([55]).

(63) Além das limitações contidas no *schedule 2* do DPA 2018, a *section 26* da referida lei prevê uma isenção que pode ser aplicada a certas disposições do RGPD do Reino Unido e do DPA 2018 caso seja necessária para salvaguardar a segurança nacional ou para fins de defesa. Tal isenção aplica-se aos princípios da proteção de dados (exceto o princípio da licitude), às obrigações de transparência, aos direitos do titular dos dados, à obrigação de notificar uma

([46]) *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.

([47]) *Guriev/Community Safety Development (United Kingdom) Ltd* [2016] EWHC 643 (QB), n.º 43. Ver também *Lin/Commissioner of Police for the Metropolis* [2015] EWHC 2484 (QB), n.º 80.

([48]) *Schedule 2*, n.º 2, do DPA 2018.

([49]) *Schedule 2*, n.º 19, do DPA 2018.

([50]) *Schedule 2*, n.º 20, do DPA 2018.

([51]) *Schedule 2*, n.º 21, do DPA 2018.

([52]) Por exemplo, as limitações ao direito à notificação de uma violação de dados só são permitidas no que respeita à criminalidade e à tributação (*schedule 2*, n.º 2, do DPA 2018), ao privilégio parlamentar (*schedule 2*, n.º 13, do DPA 2018), e ao tratamento para fins jornalísticos, académicos, artísticos e literários (*schedule 2*, n.º 26, do DPA 2018).

([53]) *Schedule 2*, n.º 2, do DPA 2018.

([54]) *R (Lord)/Secretary of State for the Home Department* [2003] EWHC 2073 (Admin), n.º 100, e *Guriev/Community Safety Development (United Kingdom) Ltd* [2016] EWHC 643 (QB), n.º 43.

([55]) *Open Rights Group & Anor, R (On the Application Of)/Secretary of State for the Home Department & Anor,* n.º 31.

violação de dados, às regras sobre transferências internacionais, a alguns dos deveres e poderes do comissário para a informação, e às regras sobre vias de recurso, responsabilidades e sanções, exceto a disposição sobre as condições gerais para a aplicação de coimas prevista no artigo 83.º do RGPD do Reino Unido e a disposição sobre sanções do artigo 84.º do RGPD do Reino Unido. Além disso, a *section 28* do DPA 2018 altera a aplicação do artigo 9.º, n.º 1, para permitir o tratamento de categorias especiais de dados no artigo 9.º, n.º 1, do RGPD do Reino Unido, na medida em que o tratamento seja efetuado para salvaguardar a segurança nacional ou para fins de defesa, e com garantias adequadas para os direitos e liberdades dos titulares dos dados ([56]).

(64) A isenção só pode ser aplicada na medida em que seja necessária para salvaguardar a segurança ou defesa nacional. Como as outras isenções previstas pelo DPA 2018, deve ser considerada e invocada pelo responsável pelo tratamento numa base casuística. Além disso, qualquer aplicação da isenção deve estar em conformidade com as normas em matéria de direitos humanos (sustentadas pelo *Human Rights Act 1998*), segundo as quais qualquer ingerência nos direitos de privacidade deve ser necessária e proporcionada numa sociedade democrática ([57]).

(65) Esta interpretação da isenção é confirmada pelo ICO, que emitiu orientações pormenorizadas sobre a aplicação da isenção relativa à defesa e à segurança nacional, clarificando que deve ser analisada e aplicada pelo responsável pelo tratamento numa base casuística ([58]). Em especial, as orientações sublinham que «[n]ão se trata de uma isenção geral» e que, a fim de a invocar, «não basta que os dados sejam tratados para fins de segurança nacional». Em contrapartida, o responsável pelo tratamento que a invoque deve «demonstrar que existe uma possibilidade real de efeitos adversos na segurança nacional» e, quando necessário, espera-se que o responsável pelo tratamento «faculte [ao ICO] elementos de prova sobre as razões pelas quais utilizou esta isenção». As orientações incluem uma lista de controlo e uma série de exemplos a fim de clarificar melhor as condições em que esta isenção pode ser invocada.

(66) Por conseguinte, o facto de os dados serem tratados para fins de segurança ou defesa nacional não é, por si só, suficiente para que a isenção seja aplicada. O responsável pelo tratamento tem de considerar as consequências reais para a segurança nacional se tivesse de cumprir a disposição específica em matéria de proteção de dados. A isenção só pode ser aplicada às disposições específicas que tenham sido identificadas como apresentando o risco e tem de ser aplicada da forma mais restritiva possível ([59]).

(67) Esta abordagem foi confirmada pelo *Information Tribunal* (tribunal especializado em questões de informação) ([60]). No processo *Baker/Secretary of State for the Home Department* («*Baker/Secretary of State*»), o tribunal determinou que era ilegal aplicar a isenção relativa à segurança nacional como uma isenção geral aos pedidos de acesso recebidos pelos serviços de informações. Em vez disso, a isenção tinha de ser aplicada caso a caso, analisando cada pedido em função do seu mérito e tendo em conta o direito das pessoas ao respeito pela sua vida privada ([61]).

([56]) De acordo com as informações fornecidas pelas autoridades do Reino Unido, quando o tratamento se insere no contexto da segurança nacional, os responsáveis pelo tratamento aplicarão normalmente garantias e medidas de segurança reforçadas ao tratamento, que reflitam a natureza sensível do mesmo. As garantias adequadas a aplicar dependerão dos riscos colocados pelo tratamento a efetuar. Poderão incluir limitações ao acesso aos dados para que apenas as pessoas que possuam autorizações de segurança adequadas tenham acesso aos mesmos, limitações rigorosas à partilha dos dados, e o elevado nível de segurança aplicado aos procedimentos de conservação e tratamento.

([57]) 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.

([58]) 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/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/national-security-and-defence/

([59]) De acordo com um exemplo fornecido pelas autoridades do Reino Unido, se um suspeito de terrorismo sob investigação ativa do MI5 tivesse apresentado um pedido de acesso ao Ministério da Administração Interna (por exemplo, por estar envolvido num litígio com o Ministério da Administração Interna sobre questões de imigração), seria necessário proteger da divulgação ao titular dos dados quaisquer dados que o MI5 pudesse ter partilhado com o Ministério da Administração Interna relativos a investigações em curso que pudessem prejudicar fontes sensíveis, métodos ou técnicas e/ou levar a um aumento da ameaça colocada pela pessoa. Nessas circunstâncias, é provável que o limiar para aplicar a isenção da *section 26* tivesse sido atingido e seria necessária uma isenção da divulgação das informações para salvaguardar a segurança nacional. No entanto, se o Ministério da Administração Interna também dispusesse de dados pessoais sobre a pessoa que não estivessem relacionados com a investigação do MI5, e se a informação pudesse ser fornecida sem risco de danos para a segurança nacional, então a isenção relativa à segurança nacional não seria aplicável na consideração da divulgação de informações à pessoa. O ICO está a elaborar orientações sobre como os responsáveis pelo tratamento devem abordar a utilização da isenção constante da *section 26*, que deverão ser publicadas até ao final de março de 2021.

([60]) O *Information Tribunal* foi criado para apreciar os recursos em matéria de proteção de dados ao abrigo do *Data Protection Act 1984*. Em 2010, passou a fazer parte da *General Regulatory Chamber* (secção de regulação geral) do *First-tier Tribunal* (tribunal de primeira instância), como parte da reforma da estrutura do sistema de tribunais do Reino Unido.

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

2.5.6 *Limitações para dados pessoais tratados para fins jornalísticos, artísticos, académicos e literários, bem como de arquivo e de investigação*

(68) O artigo 85.º, n.º 2, do RGPD do Reino Unido permite que se preveja que os dados pessoais tratados para fins jornalísticos, artísticos, académicos e literários estejam isentos de várias disposições do RGPD do Reino Unido. O *schedule 2*, parte 5, do DPA 2018 estabelece as isenções para o tratamento para estes fins. Prevê isenções dos princípios da proteção de dados (exceto do princípio de integridade e confidencialidade), dos fundamentos jurídicos para o tratamento (incluindo as categorias especiais de dados e os dados relativos a condenações penais, etc.), das condições de consentimento, das obrigações de transparência, dos direitos dos titulares dos dados, da obrigação de notificar violações de dados, do requisito de consultar o comissário para a informação antes do tratamento de elevado risco, e das regras relativas às transferências internacionais ([62]). A este respeito, o RGPD do Reino Unido não se afasta de forma significativa do Regulamento (UE) 2016/679, que no seu artigo 85.º também prevê a possibilidade de isentar o tratamento efetuado para fins jornalísticos ou de expressão académica, artística ou literária de vários requisitos do Regulamento (UE) 2016/679. As disposições do DPA 2018, nomeadamente o *schedule 2*, parte 5, são compatíveis com o RGPD do Reino Unido.

(69) O exercício de equilíbrio essencial a realizar ao abrigo do artigo 85.º do RGPD do Reino Unido está relacionado com a questão de saber se uma isenção das regras relativas à proteção de dados referida no considerando 68 é «necessária para conciliar o direito à proteção de dados pessoais com a liberdade de expressão e de informação» ([63]). De acordo com o *schedule 2*, n.º 26, pontos 2 e 3, do DPA 2018, o Reino Unido aplica um critério de «convicção razoável» para que este equilíbrio seja alcançado. Para que uma isenção seja justificada, o responsável pelo tratamento deve estar razoavelmente convicto de que i) a publicação é do interesse público; e que ii) a aplicação da disposição aplicável do RGPD seria incompatível com os fins jornalísticos, académicos, artísticos ou literários. Como confirmado pela jurisprudência ([64]), o critério da «convicção razoável» tem uma componente subjetiva e uma componente objetiva: não basta que o responsável pelo tratamento esteja convicto de que o cumprimento era incompatível. A sua convicção tem de ser razoável, ou seja, tem de poder ser partilhada por uma pessoa razoável, que conheça os factos pertinentes. Por conseguinte, o responsável pelo tratamento deve exercer a diligência devida ao formar a sua convicção, a fim de conseguir demonstrar razoabilidade. De acordo com as explicações fornecidas pelas autoridades do Reino Unido, o critério da «convicção razoável» deve ser aplicado a cada isenção ([65]). Se as condições estiverem cumpridas, a isenção é considerada necessária e proporcionada nos termos do direito do Reino Unido.

(70) Nos termos da *section 124* do DPA 2018, o ICO deve elaborar um código de boas práticas sobre o jornalismo e a proteção de dados. Os trabalhos relativos a este código estão em curso. Foram emitidas orientações sobre a matéria ao abrigo do *Data Protection Act 1998*, que salientam, nomeadamente, que, para se poder invocar esta isenção, não basta afirmar simplesmente que o cumprimento seria um inconveniente para as atividades jornalísticas, devendo existir um argumento claro de que a disposição em causa apresenta um obstáculo ao

([62]) Ver o artigo 85.º do RGPD do Reino Unido e o *schedule 2*, parte 5, n.º 26, ponto 9, do DPA 2018.

([63]) De acordo com o *schedule 2*, parte 5, n.º 26, ponto 2, do DPA 2018, a exceção aplica-se ao tratamento de dados pessoais efetuado para fins especiais (jornalísticos, académicos, artísticos e literários), se efetuado com vista à publicação de material jornalístico, académico, artístico ou literário, e se o responsável pelo tratamento estiver razoavelmente convicto de que a publicação desse material seria de interesse público. Ao determinar se uma publicação seria do interesse público, o responsável pelo tratamento tem de ter em conta a importância especial do interesse público na liberdade de expressão e de informação. Deve também ter em consideração os códigos de boas práticas ou as orientações pertinentes para a publicação em questão [as orientações editoriais da BBC (*BBC Editorial Guidelines*), o código de radiodifusão da Ofcom (*Ofcom Broadcasting Code*), e o código de boas práticas dos editores (*Editors' Code of Practice*)]. Além disso, para que uma isenção seja aplicável, o responsável pelo tratamento tem de estar razoavelmente convicto de que o cumprimento da disposição aplicável seria incompatível com os fins especiais (*schedule 2*, n.º 26, ponto 3, do DPA 2018).

([64]) O acórdão no processo *NT1/Google* [2018] EWHC 799 (QB), n.º 102, abordou uma discussão sobre se o responsável pelo tratamento de dados tinha uma convicção razoável de que a publicação era do interesse público, e de que o cumprimento das disposições aplicáveis era incompatível com os fins especiais. O tribunal observou que as *sections 32(1) (b)* e *(c)* do *Data Protection Act 1998* tinham um elemento subjetivo e um elemento objetivo: o responsável pelo tratamento tinha de estabelecer a sua convicção de que a publicação seria do interesse público, e que tal convicção era objetivamente razoável; tinha também de estabelecer uma convicção subjetiva de que o cumprimento da disposição relativamente à qual procurava a isenção seria incompatível com a finalidade especial em causa.

([65]) Um exemplo de como é aplicado o critério da «convicção razoável» está incluído na decisão do ICO de multar a True Visions Productions, que foi tomada ao abrigo do *Data Protection Act 1998*. O ICO aceitou que o responsável pelo controlo dos meios de comunicação social tinha uma convicção subjetiva de que o cumprimento do primeiro princípio da proteção de dados (lealdade e licitude) era incompatível com os fins jornalísticos. No entanto, não aceitou que tal convicção era objetivamente razoável. A decisão do ICO pode ser consultada na seguinte ligação: https://ico.org.uk/media/action-weve-taken/mpns/2614746/true-visions-productions-20190408.pdf

jornalismo responsável ([66]). A entidade reguladora das telecomunicações do Reino Unido, OFCOM, e a BBC, nas suas orientações editoriais, também publicaram orientações relativas à aplicação do critério de interesse público e ao equilíbrio entre o interesse público e o interesse individual na privacidade ([67]). Em particular, tais orientações dão exemplos de informações que podem ser consideradas de interesse público, e explicam a necessidade de poder demonstrar que o interesse público prevalece relativamente aos direitos à privacidade nas circunstâncias específicas do caso.

(71) Conforme previsto no artigo 89.º do RGPD, os dados pessoais tratados para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos também podem ser isentos de várias disposições do RGPD do Reino Unido, devidamente especificadas ([68]). No que respeita à investigação e à produção de estatísticas, são possíveis isenções às disposições do RGPD do Reino Unido relacionadas com a confirmação do tratamento, o acesso aos dados e as garantias para transferências de países terceiros, o direito de retificação, a limitação do tratamento e a objeção ao tratamento. No que respeita ao arquivo de interesse público, são também possíveis isenções da obrigação de notificação da retificação ou apagamento dos dados pessoais ou limitação do tratamento e do direito de portabilidade dos dados.

(72) Nos termos do *schedule 2*, n.º 27, ponto 1, e n.º 28, ponto 1, do DPA 2018, as isenções das disposições indicadas do RGPD do Reino Unido são possíveis sempre que a aplicação dessas disposições «impeça ou prejudique gravemente a realização» dos objetivos em questão ([69]).

(73) Dada a sua relevância para um exercício efetivo dos direitos individuais, qualquer desenvolvimento pertinente no que respeita à interpretação e à aplicação prática das isenções acima referidas (para além da relativa à manutenção de um controlo efetivo da imigração, conforme explicado no considerando 6), incluindo qualquer desenvolvimento futuro da jurisprudência e das orientações e medidas de execução do ICO, será devidamente tida em conta no contexto do controlo contínuo da presente decisão ([70]).

2.5.7 *Restrições relativas a transferências ulteriores*

(74) O nível de proteção conferido aos dados pessoais transferidos da União Europeia para responsáveis pelo tratamento ou subcontratantes no Reino Unido não pode ser prejudicado pela transferência subsequente desses dados para destinatários num país terceiro. As referidas «transferências ulteriores», que constituem, da perspetiva do responsável pelo tratamento ou subcontratante do Reino Unido, transferências internacionais do Reino Unido, apenas devem ser permitidas nos casos em que o destinatário fora do Reino Unido esteja, pelo seu lado, sujeito a normas que assegurem um nível de proteção semelhante ao garantido no âmbito da ordem jurídica do Reino Unido. Por esse motivo, a aplicação das regras do RGPD do Reino Unido e do DPA 2018 relativas às transferências internacionais de dados pessoais constituem um fator importante para garantir a continuidade da proteção no caso dos dados pessoais transferidos da União Europeia para o Reino Unido ao abrigo da presente decisão.

([66]) De acordo com as orientações, as organizações têm de conseguir explicar por que razão o cumprimento da disposição aplicável do *Data Protection Act 1998* é incompatível com os fins do jornalismo. Em particular, os responsáveis pelo tratamento têm de equilibrar o efeito prejudicial que o cumprimento teria no jornalismo com o efeito prejudicial que o incumprimento teria nos direitos do titular dos dados. Se um jornalista conseguir, razoavelmente, atingir os seus objetivos editoriais de uma forma que esteja em conformidade com as disposições normalizadas do DPA, tem de o fazer. As organizações têm de conseguir justificar a sua utilização da limitação relativamente a cada disposição que não tenham cumprido. *Data protection and journalism: a guide for the media* (Proteção de dados e jornalismo: um guia para os meios de comunicação social), disponível na seguinte ligação: https://ico.org.uk/media/for-organisations/documents/1552/data-protection-and-journalism-media-guidance.pdf

([67]) Exemplos do interesse público incluiriam revelar ou detetar crimes, proteger a saúde pública ou a segurança, expor declarações enganosas feitas por indivíduos ou organizações ou revelar incompetência que afete o público. Ver o guia da OFCOM, disponível na seguinte ligação: https://www.ofcom.org.uk/__data/assets/pdf_file/0017/132083/Broadcast-Code-Section-8.pdf, e as orientações editoriais da BBC, disponíveis na seguinte ligação: https://www.bbc.com/editorialguidelines/guidelines/privacy

([68]) Ver o artigo 89.º do RGPD do Reino Unido e o *schedule 2*, parte 6, n.º 27, ponto 2, e n.º 28, ponto 2, do DPA 2018.

([69]) Sujeito à obrigação de os dados pessoais serem tratados nos termos do artigo 89.º, n.º 1, do RGPD do Reino Unido, conforme completado pela *section 19* do DPA 2018.

([70]) Ver os considerandos 281 a 287.

(75) O regime relativo às transferências internacionais de dados pessoais do Reino Unido é estabelecido nos artigos 44.º a 49.º do RGPD do Reino Unido, completado pelo DPA 2018, e é, em substância, idêntico às regras previstas no capítulo V do Regulamento (UE) 2016/679 ([71]). As transferências de dados pessoais para países terceiros ou organizações internacionais só podem ser efetuadas se existirem regulamentos de adequação [o equivalente do Reino Unido a uma decisão de adequação ao abrigo do Regulamento (UE) 2016/679] ou, na falta de regulamentos de adequação, caso o responsável pelo tratamento ou o subcontratante tenha apresentado garantias adequadas nos termos do artigo 46.º do RGPD do Reino Unido. Na falta de regulamentos de adequação ou de garantias adequadas, uma transferência só pode ser efetuada com base nas derrogações estabelecidas no artigo 49.º do RGPD do Reino Unido.

(76) Os regulamentos de adequação efetuados pelo ministro da tutela podem estipular que um país terceiro (ou território ou setor de um país terceiro), uma organização internacional ou uma descrição ([72]) desse país, território, setor, ou organização assegura um nível adequado de proteção de dados pessoais. Ao avaliar a adequação do nível de proteção, o ministro da tutela deve ter em conta exatamente os mesmos elementos que a Comissão é obrigada a avaliar, ao abrigo do artigo 45.º, n.º 2, alíneas a) a c), do Regulamento (UE) 2016/679, interpretado em conjunto com o considerando 104 do Regulamento (UE) 2016/679 e a jurisprudência da UE mantida. Tal significa que, ao avaliar a adequação do nível de proteção de um país terceiro, a norma pertinente será se esse país terceiro em questão assegura um nível de proteção «essencialmente equivalente» ao assegurado no Reino Unido.

(77) Quanto ao procedimento, os regulamentos de adequação estão sujeitos aos requisitos processuais «gerais» previstos na *section 182* do DPA 2018. 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 ([73]). 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 escrutinar os regulamentos e podem aprovar uma moção para anular os regulamentos no prazo de 40 dias ([74]).

(78) Nos termos da *section 17B(1)* do DPA 2018, os regulamentos de adequação devem ser revistos em intervalos não superiores a quatro anos e o ministro da tutela deve controlar, de forma continuada, os desenvolvimentos nos países terceiros e nas organizações internacionais que possam afetar as decisões que visam criar regulamentos de adequação ou alterar ou revogar esses regulamentos. Caso tenha conhecimento de que um país ou organização específico deixou de assegurar um nível adequado de proteção de dados pessoais, o ministro da tutela deve, na medida do necessário, alterar ou revogar os regulamentos e iniciar consultas com o país terceiro ou a organização internacional em causa com vista a corrigir a falta de um nível adequado de proteção. Estes aspetos processuais refletem igualmente os requisitos correspondentes previstos no Regulamento (UE) 2016/679.

([71]) Com a exceção do artigo 48.º do Regulamento (UE) 2016/679, que o Reino Unido decidiu não incluir no RGPD do Reino Unido. A este respeito, em primeiro lugar importa recordar que a norma a considerar como proporcionando um nível de proteção adequado é uma norma de «equivalência essencial» e não de identidade, conforme clarificado pelo TJUE (Schrems I, n.ºs 73 e 74) e reconhecido pelo CEPD (documento de referência relativo à adequação, p. 3). Por conseguinte, conforme explicado pelo CEPD no seu documento de referência relativo à adequação, «o objetivo não é imitar ponto por ponto a legislação europeia, mas sim estabelecer o essencial — os principais requisitos dessa legislação». A este respeito, importa notar que, embora a ordem jurídica do Reino Unido não inclua formalmente uma disposição idêntica ao artigo 48.º, o mesmo efeito é garantido por outras disposições e princípios jurídicos, ou seja, que, em resposta a um pedido de dados pessoais apresentado por um tribunal ou por uma autoridade administrativa de um país terceiro, os dados pessoais só podem ser transferidos para esse país terceiro se existir um acordo internacional em vigor — com base no qual a decisão judicial ou administrativa do país terceiro em questão é reconhecida ou executada no Reino Unido — ou se a transferência se basear num dos mecanismos de transferência previstos no capítulo V do RGPD do Reino Unido. Mais especificamente, de modo a executar uma sentença estrangeira, os tribunais do Reino Unido devem ser capazes de nomear um direito comum ou um estatuto que permita a sua executividade. Todavia, nem o direito comum (ver *Adams and Others/Cape Industries Plc.*, [1990] 2 W.L.R. 657) nem os estatutos garantem a execução das sentenças estrangeiras que exigem a transferência de dados sem a existência de um acordo internacional. Consequentemente, os pedidos de dados não são executáveis ao abrigo do direito do Reino Unido, na ausência de tal acordo internacional. Além disso, qualquer transferência de dados pessoais para países terceiros — incluindo a pedido de um tribunal estrangeiro ou de uma autoridade administrativa estrangeira — permanece sujeita às restrições estabelecidas no capítulo V do RGPD do Reino Unido, que são idênticas às disposições correspondentes do Regulamento (UE) 2016/679, e, por conseguinte, necessitam de recorrer a um dos motivos de transferência previstos no capítulo V, em conformidade com as condições específicas a que estão sujeitas ao abrigo desse capítulo.

([72]) As autoridades do Reino Unido explicaram que a descrição de um país ou de uma organização internacional diz respeito a uma situação em que seria necessário realizar uma determinação específica e parcial da adequação com restrições orientadas (por exemplo, regulamentos de adequação relativos apenas a determinados tipos de transferências de dados).

([73]) 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

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

(79) Na falta de regulamentos de adequação, podem ser efetuadas transferências internacionais se os responsáveis pelo tratamento ou subcontratantes tiverem apresentado garantias adequadas, nos termos do artigo 46.º do RGPD do Reino Unido. Essas garantias são semelhantes às previstas no artigo 46.º do Regulamento (UE) 2016/679. Incluem instrumentos juridicamente vinculativos e com força executiva entre autoridades ou organismos públicos, regras vinculativas aplicáveis às empresas ([75]), cláusulas-tipo de proteção de dados, códigos de conduta aprovados, procedimentos de certificação aprovados e, com a autorização do comissário para a informação, cláusulas contratuais entre os responsáveis pelo tratamento (ou os subcontratantes) ou acordos administrativos entre as autoridades públicas. Contudo, as regras foram modificadas, de um ponto de vista processual, para se adequarem ao quadro do Reino Unido. Em particular, as cláusulas-tipo de proteção de dados podem ser adotadas pelo ministro da tutela (*section 17C*) ou pelo comissário para a informação (*section 119A*), em conformidade com o DPA 2018.

(80) Na falta de uma decisão de adequação ou de garantias adequadas, uma transferência só pode ser efetuada com base nas derrogações estabelecidas no artigo 49.º do RGPD do Reino Unido ([76]). O RGPD do Reino Unido não introduz alterações significativas às derrogações, em comparação com as regras correspondentes do Regulamento (UE) 2016/679. Ao abrigo do RGPD do Reino Unido, tal como disposto no Regulamento (UE) 2016/679, apenas se pode recorrer a determinadas derrogações se a transferência for ocasional ([77]). Além disso, o ICO, nas suas orientações sobre transferências internacionais, esclarece que: «[e]stas apenas devem ser utilizadas como "exceções" verdadeiras da regra geral e não deve ser efetuada uma transferência restrita a não ser que se encontre abrangida por uma decisão de adequação ou que existam garantias adequadas» ([78]). No que diz respeito às transferências que são necessárias por importantes razões de interesse público [artigo 49.º, n.º 1, alínea d)], o ministro da tutela pode efetuar regulamentos para especificar as circunstâncias nas quais uma transferência de dados pessoais para um país terceiro ou uma organização internacional não é necessária por razões importantes de interesse público. Além disso, o ministro da tutela pode, por meio de regulamentos, restringir a transferência de uma categoria de dados pessoais para um país terceiro ou uma organização internacional caso não seja possível efetuar a transferência com base nos regulamentos de adequação e o ministro da tutela considere a restrição necessária por importantes razões de interesse público. Até ao momento, não foram adotados esses regulamentos.

(81) Este quadro para transferências internacionais tornou-se aplicável no final do período de transição ([79]). Contudo, o *schedule 21*, n.º 4, do DPA 2018 (introduzido pelos Regulamentos DPPEC) prevê que, no fim do período de transição, determinadas transferências de dados pessoais sejam tratadas como se fossem baseadas em regulamentos de adequação, o que inclui transferências para um Estado do EEE, o território de Gibraltar, uma instituição, órgão, organismo ou agência da União criado por um Tratado da UE ou com base num tratado dessa natureza e para

([75]) O RGPD do Reino Unido mantém as regras previstas no artigo 47.º do Regulamento (UE) 2016/679 sujeitas apenas a modificações para enquadrarem as regras no contexto nacional, por exemplo, substituindo as referências à autoridade de controlo competente pelo comissário para a informação, eliminando a referência ao procedimento de controlo da coerência previsto no n.º 1 e eliminando todo o n.º 3.

([76]) Nos termos do artigo 49.º do RGPD do Reino Unido, as transferências podem ser efetuadas se for cumprida uma das seguintes condições: a) o titular dos dados tiver explicitamente dado o seu consentimento à transferência prevista, após ter sido informado dos possíveis riscos de tais transferências para si próprio devido à falta de uma decisão de adequação e das garantias adequadas; b) a transferência for necessária para a execução de um contrato entre o titular dos dados e o responsável pelo tratamento ou de diligências prévias à formação do contrato decididas a pedido do titular dos dados; c) a transferência for necessária para a celebração ou execução de um contrato, celebrado no interesse do titular dos dados, entre o responsável pelo seu tratamento e outra pessoa singular ou coletiva; d) a transferência for necessária por importantes razões de interesse público; e) a transferência for necessária à declaração, ao exercício ou à defesa de um direito num processo judicial; f) a transferência for necessária para proteger interesses vitais do titular dos dados ou de outras pessoas, se esse titular estiver física ou legalmente incapaz de dar o seu consentimento; d) a transferência for realizada a partir de um registo que, nos termos do direito nacional, se destine a informar o público e se encontre aberto à consulta do público em geral ou de qualquer pessoa que possa provar nela ter um interesse legítimo, mas apenas na medida em que as condições de consulta estabelecidas no direito nacional se encontrem preenchidas nesse caso concreto. Além disso, caso não se aplique nenhuma das condições supramencionadas, uma transferência só pode ser efetuada se não for repetitiva, apenas disser respeito a um número limitado de titulares de dados, for necessária para efeitos de interesses legítimos visados pelo responsável pelo seu tratamento, desde que a tais interesses não se sobreponham os interesses ou os direitos e liberdades do titular dos dados, e o responsável pelo tratamento tiver ponderado todas as circunstâncias relativas à transferência de dados e, com base nessa avaliação, tiver apresentado garantias adequadas no que respeita à proteção de dados pessoais.

([77]) O considerando 111 do RGPD do Reino Unido especifica que as transferências relativas a um contrato ou a um contencioso judicial só podem ser efetuadas se forem ocasionais.

([78]) Orientações do ICO sobre transferências internacionais, disponível na seguinte ligação: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers/#ib7

([79]) Durante um período de, no máximo, seis meses, que termina o mais tardar em 30 de junho de 2021, a aplicabilidade deste quadro novo deve ser lida à luz do 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 (JO L 444 de 31.12.2020, p. 14) («Acordo de Comércio e Cooperação UE-RU»), disponível na seguinte ligação: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:22020A1231(01)&from=EN

países terceiros que foram objeto de uma decisão de adequação da UE no final do período de transição. Consequentemente, as transferências para esses países podem continuar como ocorria anteriormente à saída do Reino Unido da UE. Após o fim do período de transição, o ministro da tutela deve proceder a uma análise destas conclusões de adequação durante um período de quatro anos, ou seja, até ao final de dezembro de 2024. De acordo com a explicação apresentada pelas autoridades do Reino Unido, embora seja necessário que o ministro da tutela efetue essa análise até ao final de dezembro de 2024, as disposições transitórias não incluem uma disposição «de caducidade» e as disposições transitórias aplicáveis não deixarão automaticamente de ter efeito se a análise não for concluída até ao final de dezembro de 2024.

(82) Por último, no que diz respeito à evolução futura do regime de transferências internacionais do Reino Unido — através da adoção de novos regulamentos de adequação, da celebração de acordos internacionais ou do desenvolvimento de outros mecanismos de transferência —, a Comissão acompanhará de perto a situação, avaliará se os diferentes mecanismos de transferência são utilizados de forma a assegurar a continuidade da proteção e, se necessário, tomará as medidas adequadas a fim de dar resposta a eventuais efeitos adversos para tal continuidade (ver os considerandos 278 a 287). Uma vez que a UE e o Reino Unido partilham regras semelhantes em matéria de transferências internacionais, espera-se que possam igualmente ser evitadas divergências problemáticas através da cooperação, do intercâmbio de informações e da partilha de experiências, nomeadamente entre o ICO e o CEPD.

2.5.8 *Responsabilidade*

(83) De acordo com o princípio da responsabilidade, as entidades responsáveis pelo tratamento de dados são obrigadas a aplicar medidas técnicas e organizativas adequadas para cumprir as suas obrigações de proteção dos dados de forma eficaz e poder demonstrar esse cumprimento, em particular junto da autoridade de controlo competente.

(84) O princípio da responsabilidade previsto no Regulamento (UE) 2016/679 foi mantido no artigo 5.º, n.º 2, do RGPD do Reino Unido, sem alterações significativas, e o mesmo se aplica ao artigo 24.º, que diz respeito à responsabilidade do responsável pelo tratamento, ao artigo 25.º, que diz respeito à proteção de dados desde a conceção e por defeito, e ao artigo 30.º, que diz respeito aos registos das atividades de tratamento. Os artigos 35.º e 36.º, relativos à avaliação de impacto sobre a proteção de dados e à consulta prévia por parte da autoridade de controlo, também foram mantidos. Os artigos 37.º e 39.º do Regulamento (UE) 2016/679 relativos à designação e às funções do encarregado da proteção de dados foram mantidos no RGPD do Reino Unido sem alterações significativas. Além disso, as disposições dos artigos 40.º e 42.º do Regulamento (UE) 2016/679 relativos aos códigos de conduta e à certificação foram mantidas no RGPD do Reino Unido ([80]).

2.6 **Supervisão e execução coerciva**

2.6.1 *Supervisão independente*

(85) Por forma a assegurar que seja garantido na prática um nível adequado de proteção dos dados, deve ser criada uma autoridade de controlo independente incumbida de supervisionar e executar coercivamente as normas em matéria de proteção de dados. Essa autoridade deve atuar com total independência e imparcialidade no cumprimento das suas obrigações e no exercício das respetivas competências.

(86) No Reino Unido, é o comissário para a informação quem efetua a supervisão e a execução coerciva do cumprimento do RGPD do Reino Unido e do DPA 2018. O comissário para a informação é uma «sociedade individual»: uma entidade jurídica separada composta por uma pessoa singular. O comissário para a informação é apoiado no seu trabalho por um gabinete. Em 31 de março de 2020, o Gabinete do Comissário para a Informação tinha 768 membros permanentes ([81]). O departamento que patrocina o comissário para a informação é o Ministério dos Assuntos Digitais, da Cultura, dos Meios de Comunicação e do Desporto ([82]).

(87) A independência do comissário é descrita explicitamente no artigo 52.º do RGPD do Reino Unido, que não efetua quaisquer alterações significativas ao artigo 52.º, n.ºs 1 a 3, do RGPD. Nos termos do RGPD do Reino Unido, o comissário deve agir com total independência na prossecução das suas atribuições e no exercício dos poderes que lhe são atribuídos, não deve estar sujeito a influências externas, diretas ou indiretas no desempenho das suas

([80]) Se necessário, estas referências são substituídas por referências às autoridades do Reino Unido. Por exemplo, nos termos da *section 17* do DPA 2018, o comissário para a informação ou o organismo nacional de acreditação do Reino Unido pode acreditar uma pessoa que reúna os requisitos estabelecidos no artigo 43.º do RGPD do Reino Unido para que esta supervisione o cumprimento de uma certificação.

([81]) *Information Commissioner's Annual Report and Financial Statements 2019-2020* (Relatório anual e demonstrações financeiras do comissário para a informação), disponível na seguinte ligação: https://ico.org.uk/media/about-the-ico/documents/2618021/annual-report-2019-20-v83-certified.pdf

([82]) Um acordo de gestão regula a relação entre os dois. Em particular, as responsabilidades principais do Ministério dos Assuntos Digitais, da Cultura, dos Meios de Comunicação e do Desporto, enquanto departamento patrocinador, incluem: garantir que o comissário para a informação recebe financiamento e os recursos adequados; representar os interesses do comissário para a informação junto do parlamento e de outros departamentos governamentais; garantir a existência de um quadro nacional de proteção de dados sólido; e prestar orientações e apoio ao Gabinete do Comissário para a Informação em questões empresariais, como mercado imobiliário, locações e aquisições (Acordo de Gestão para 2018-2021, disponível na seguinte ligação: https://ico.org.uk/media/about-the-ico/documents/2259800/management-agreement-2018-2021.pdf)

funções e no exercício dos seus poderes e não deve solicitar nem receber instruções de ninguém. O comissário deve igualmente abster-se de qualquer ato incompatível com as suas funções e, durante o seu mandato, não pode desempenhar nenhuma atividade, remunerada ou não, que com elas seja incompatível.

(88) As condições para a nomeação e a exoneração do comissário para a informação estão estabelecidas no *schedule 12* do DPA 2018. O comissário para a informação é nomeado por Sua Majestade com base numa recomendação do governo, na sequência de um concurso equitativo e aberto. O candidato deve ter as qualificações, as competências e as aptidões adequadas. De acordo com o *Governance Code on Public Appointments* ([83]), o painel de avaliação consultiva efetua uma lista dos candidatos que podem ser nomeados. Antes de o ministro da tutela do Ministério dos Assuntos Digitais, da Cultura, dos Meios de Comunicação e do Desporto concluir a sua decisão, a comissão especial competente do parlamento deve realizar uma triagem prévia à nomeação. A posição da comissão é tornada pública ([84]).

(89) O mandato do comissário para a informação dura, no máximo, sete anos. Uma pessoa não pode ser nomeada comissário para a informação mais do que uma vez. O comissário para a informação pode ser afastado do mandato por Sua Majestade na sequência de um comunicado de ambas as câmaras do parlamento ([85]). Não pode ser apresentado nenhum pedido de exoneração do comissário para a informação a nenhuma das câmaras do parlamento a não ser que um ministro tenha apresentado um relatório onde indique que está convicto de que o comissário para a informação cometeu uma falta grave e/ou que o comissário deixou de cumprir as condições exigidas para o exercício das suas funções ([86]).

(90) O financiamento do comissário para a informação é proveniente de três fontes: i) taxas em matéria de proteção de dados pagas pelos responsáveis pelo tratamento, que são fixadas pelos regulamentos do ministro da tutela ([87]) (o *Data Protection (Charges and Information) Regulations 2018* [Regulamentos de 2018 relativos à Proteção de Dados (taxas e informações)], e correspondem entre 85% a 90% do orçamento anual do gabinete ([88]); ii) subvenção de Estado paga pelo governo ao comissário para a informação. A subvenção de Estado é maioritariamente utilizada para financiar os custos de operação do comissário para a informação no que diz respeito a funções não relacionadas com a proteção de dados ([89]); e iii) taxas cobradas pelos serviços ([90]). De momento, essas taxas não são cobradas.

(91) As funções gerais do comissário para a informação relativas ao tratamento de dados pessoais aos quais se aplica o RGPD do Reino Unido são estabelecidas no artigo 57.º do mesmo e refletem as regras correspondentes previstas no Regulamento (UE) 2016/679. As suas funções incluem o controlo e a execução do RGPD do Reino Unido, a promoção da sensibilização do público, o tratamento de reclamações apresentadas pelos titulares dos dados, a realização de investigações, etc. Além disso, a *section 115* do DPA 2018 estabelece outras funções gerais do comissário, que incluem um dever de aconselhar o parlamento, o governo e outras instituições e organismos a respeito das medidas legislativas e administrativas relacionadas com a defesa dos direitos e liberdades das pessoas singulares no que diz respeito ao tratamento de dados pessoais e um poder para emitir, por iniciativa própria do comissário ou se lhe for solicitado, pareceres dirigidos ao parlamento, ao governo ou a outras instituições e

([83]) *Governance Code on Public Appointments* (código para a governação das nomeações públicas), disponível na seguinte ligação: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/578498/governance_code_on_public_appointments_16_12_2016.pdf

([84]) *Second Report of Session 2015-2016* (Segundo relatório da sessão de 2015-2016) da *Culture, Media and Sports Committee* (comissão para a cultura, os meios de comunicação e o desporto) da Câmara dos Comuns, disponível na seguinte ligação: https://publications.parliament.uk/pa/cm201516/cmselect/cmcumeds/990/990.pdf

([85]) Um «comunicado» é uma moção apresentada ao parlamento que procura informar a monarca dos pareceres do parlamento numa determinada questão.

([86]) *Schedule 12*, n.º 3, ponto 3, do DPA 2018.

([87]) *Section 137* do DPA 2018, ver considerando 17.

([88]) As *sections 137* e *138* do DPA 2018 incluem uma série de garantias para assegurar a fixação correta das taxas. Em particular, a *section 137(4)* enumera as matérias que o ministro da tutela deve ter em conta ao criar regulamentos que especificam o montante que as diferentes organizações devem pagar; Em segundo lugar, a *section 138(1)* e a *section 182* do DPA 2018 também incluem uma obrigação legal que exige que o ministro da tutela consulte o comissário para a informação e outros representantes das pessoas que são suscetíveis de serem afetadas pelos regulamentos, antes da respetiva criação, de modo a ter em conta os seus pontos de vista. Além disso, nos termos da *section 138(2)* do DPA 2018, o comissário para a informação é obrigado a manter o trabalho do *Charges Regulations* (Regulamentos relativos às Taxas) sob análise e pode apresentar propostas ao ministro da tutela para que sejam efetuadas alterações nos regulamentos. Por último, exceto nos casos em que os regulamentos são criados simplesmente para ter em conta um aumento do índice do preço de retalho (sendo que, nesse caso, serão sujeitos ao procedimento de resolução negativa), os regulamentos estão sujeitos ao procedimento de resolução afirmativa e não podem ser criados até terem sido aprovados por resolução por cada uma das câmaras do parlamento.

([89]) O Acordo de Gestão esclareceu que «[o] ministro da tutela pode efetuar pagamentos ao comissário para a informação com o dinheiro disponibilizado pelo parlamento, nos termos do *schedule 12*, n.º 9, do DPA 2018. Após consulta do comissário para a informação, o Ministério dos Assuntos Digitais, da Cultura, dos Meios de Comunicação e do Desporto irá pagar-lhe os montantes adequados (a subvenção de Estado) para os custos administrativos do ICO e o exercício das funções do comissário para a informação relativas a uma série de funções específicas, incluindo a liberdade de informação» (Acordo de Gestão para 2018-2021, secção 1.12, ver a nota de rodapé 82).

([90]) Ver a *section 134* do DPA 2018.

organismos, bem como ao público, sobre qualquer assunto relacionado com a proteção de dados pessoais. A fim de assegurar a independência do poder judicial, o comissário para a informação não está autorizado a exercer as suas funções relativas ao tratamento de dados pessoais efetuado pelos tribunais ou por pessoas singulares no exercício da sua função jurisdicional. Contudo, os organismos especializados realizam a supervisão do poder judicial (ver os considerandos 99 a 103).

2.6.2 *Execução, incluindo sanções*

(92) Os poderes do comissário para a informação são estabelecidos no artigo 58.º do RGPD do Reino Unido, que não introduz alterações significativas ao artigo correspondente do Regulamento (UE) 2016/679. O DPA 2018 estabelece regras complementares sobre como estes poderes podem ser exercidos. Em particular, o comissário tem poderes para: a) ordenar que o responsável pelo tratamento e o subcontratante (e, em determinadas circunstâncias, qualquer outra pessoa) prestem as informações necessárias mediante uma notificação informativa («notificação informativa») ([91]); b) levar a cabo investigações e auditorias através da emissão de uma notificação de avaliação, o que poderá implicar que o responsável pelo tratamento ou o subcontratante permita que o comissário entre nas instalações específicas, inspecione ou analise os documentos ou os equipamentos, entreviste as pessoas responsáveis pelo tratamento dos dados pessoais em nome do responsável pelo tratamento, etc. («notificação de avaliação») ([92]); c) obter acesso aos documentos, etc. dos responsáveis pelo tratamento e dos subcontratantes e aceder às suas instalações de acordo com a *section 154* do DPA 2018 («poderes de entrada e inspeção»); d) exercer poderes de correção, nomeadamente por meio de advertências ou repreensões ou dar ordens por meio de uma notificação de execução, que exige que os responsáveis pelo tratamento/subcontratantes tomem ou se abstenham de tomar medidas específicas, incluindo ordenar que o responsável pelo tratamento ou o subcontratante tome qualquer umas das medidas especificadas no artigo 58.º, n.º 2, alíneas c) a g) e j), do RGPD do Reino Unido («notificação de execução») ([93]); e) e emitir coimas sob a forma de uma notificação de sanção («notificação de sanção») ([94]). Estas coimas podem ser igualmente emitidas no caso de uma autoridade pública não cumprir as disposições do RGPD do Reino Unido ([95]).

(93) A política de intervenção regulamentar do ICO descreve as circunstâncias em que será emitida uma notificação informativa, de avaliação, de execução ou de sanção ([96]). Uma notificação de execução emitida em resposta a uma falha do responsável pelo tratamento ou do subcontratante apenas pode impor os requisitos que o comissário considera adequados para efeitos de correção da falha. As notificações de execução e de sanção podem ser emitidas para um responsável pelo tratamento ou um subcontratante relativamente às violações do capítulo II do RGPD do Reino Unido (princípios de tratamento), dos artigos 12.º a 22.º (direitos dos titulares dos dados), dos artigos 25.º a 39.º (obrigações dos responsáveis pelo tratamento e dos subcontratantes) e dos artigos 44.º a 49.º (transferências internacionais) do RGPD do Reino Unido. Também pode ser emitida uma notificação de execução caso um responsável pelo tratamento não cumpra o requisito de pagar uma taxa nos regulamentos efetuados ao abrigo da *section 137* do DPA 2018. Além disso, nos termos do artigo 41.º, um organismo de supervisão ou um prestador de certificação pode receber uma notificação de execução caso não cumpra as suas obrigações previstas no RGPD do Reino Unido. Uma pessoa que não tenha cumprido uma notificação informativa, uma notificação de avaliação ou uma notificação de execução pode receber uma notificação de sanção.

(94) A notificação de sanção exige que a pessoa pague um montante especificado na notificação ao comissário para a informação. Ao determinar se deverá aplicar uma notificação de sanção a uma pessoa e ao determinar o montante da sanção, o comissário para a informação deve ter em conta as matérias enumeradas no artigo 83.º, n.ºs 1 e 2, do RGPD do Reino Unido, que são idênticas às regras correspondentes do Regulamento (UE) 2016/679 ([97]). Nos termos do artigo 83.º, n.ºs 4 e 5, em caso de incumprimento das obrigações referidas nessas disposições, os

([91]) *Section 142* do DPA 2018 (sujeita às restrições previstas na *section 143* do DPA 2018).
([92]) *Section 146* do DPA 2018 (sujeita às restrições previstas na *section 147* do DPA 2018).
([93]) *Sections 149* a *151* do DPA 2018 (sujeitas às restrições previstas na *section 152* do DPA 2018).
([94]) *Section 155* do DPA 2018 e artigo 83.º do RGPD do Reino Unido.
([95]) Tal decorre da *section 155(1)* do DPA 2018, em conjugação com a *section 149(2)* e *(5)* do DPA 2018, e da *section 156(4)* do DPA 2018, que limitam a emissão de notificações de sanção apenas no que diz respeito aos *Crown Estate Commissioners* (comissários para as propriedades da Coroa) e aos responsáveis pelo tratamento para a *Royal Household* (família real), nos termos da *section 209(4)* do DPA 2018.
([96]) *Regulatory Action Policy* (política de intervenção regulamentar), disponível na seguinte ligação: https://ico.org.uk/media/about-the-ico/documents/2259467/regulatory-action-policy.pdf
([97]) Incluindo a natureza e a gravidade da infração (tendo em conta a natureza, o âmbito ou o objetivo do tratamento de dados em causa, bem como o número de titulares de dados afetados e o nível de danos por eles sofridos), o caráter intencional ou negligente da infração, a iniciativa tomada pelo responsável pelo tratamento para atenuar os danos sofridos pelos titulares, o grau de responsabilidade do responsável pelo tratamento ou do subcontratante (tendo em conta as medidas técnicas ou organizativas por eles implementadas), quaisquer infrações pertinentes anteriormente cometidas pelo responsável pelo tratamento ou pelo subcontratante; o grau de cooperação com o comissário, as categorias específicas de dados pessoais afetadas pela infração, qualquer outro fator agravante ou atenuante aplicável às circunstâncias do caso, como os benefícios financeiros obtidos ou as perdas evitadas, direta ou indiretamente, por intermédio da infração.

montantes máximos das coimas são 8 700 000 ou 17 500 000 libras esterlinas (GBP), respetivamente. No caso de uma empresa, o comissário para a informação também pode impor coimas como percentagem do seu volume de negócios anual a nível mundial, se for mais elevado. À semelhança das disposições equivalentes do Regulamento (UE) 2016/679, estes montantes estão fixados em 2% e 4% no artigo 83.º, n.ºs 4 e 5, respetivamente. Em caso de incumprimento de uma notificação informativa, de uma notificação de avaliação ou de uma notificação de execução, o montante máximo da sanção que pode ser imposto por uma notificação de sanção é superior a 17 500 000 GBP ou, no caso de uma empresa, 4% do seu volume de negócios anual a nível mundial.

(95) O RGPD do Reino Unido, em conjunto com o DPA 2018, também reforçou outros poderes do comissário para a informação. Por exemplo, o comissário pode agora levar a cabo auditorias obrigatórias sobre todos os responsáveis pelo tratamento e subcontratantes por meio de notificações de avaliação, ao passo que, na anterior legislação do *Data Protection Act 1998*, o comissário só tinha este poder relativamente ao governo central e às organizações de saúde, sendo que os outros organismos tinham de concordar com a auditoria.

(96) Desde a introdução do Regulamento (UE) 2016/679, o ICO trata cerca de 40 000 reclamações de titulares dos dados por ano ([98]) e, além disso, realiza cerca de 2 000 investigações *ex officio* ([99]). A maioria das reclamações dizem respeito aos direitos de acesso aos dados e à divulgação dos mesmos. Na sequência das suas investigações, o comissário está a adotar medidas de execução em vários setores. Mais especificamente, de acordo com o relatório anual mais recente (2019-2020) do comissário para a informação ([100]), o comissário emitiu 54 notificações informativas, 8 notificações de avaliação, 7 notificações de execução, 4 advertências, 8 ações penais e 15 coimas durante o período de comunicação ([101]).

(97) Tal inclui várias coimas financeiras avultadas, impostas ao abrigo do Regulamento (UE) 2016/679 e do DPA 2018. Em particular, em outubro de 2020, o comissário para a informação multou uma companhia aérea inglesa em 20 milhões de GBP por uma violação de dados que afetou mais de 400 000 clientes. No final de outubro de 2020, uma cadeia de hotéis internacional recebeu uma coima no valor de 18,4 milhões de GBP por não conseguir manter os dados pessoais de milhões de clientes seguros e, em novembro de 2020, um prestador de serviços inglês que vendia bilhetes para eventos em linha recebeu uma coima no valor de 1,25 milhões de GBP por não ter protegido os dados de pagamento dos clientes ([102]).

(98) Para além dos poderes de execução do comissário para a informação descritos no considerando 92, determinadas violações da legislação em matéria de proteção de dados constituem infrações e, como tal, podem ser sujeitas a sanções penais (*section 196* do DPA 2018). Tal aplica-se, por exemplo, à obtenção ou divulgação consciente ou inconsciente de dados pessoais sem o consentimento do responsável pelo tratamento, à divulgação de dados pessoais a outra pessoa sem o consentimento do responsável pelo tratamento ([103]), à reidentificação de informações que são dados pessoais anonimizados sem o consentimento do responsável pelo tratamento que ficou incumbido da anonimização dos dados pessoais ([104]), à obstrução intencional do poder do comissário de exercer os seus poderes relativamente à inspeção dos dados pessoais, de acordo com as obrigações internacionais ([105]), às declarações falsas em resposta a uma notificação informativa ou à destruição de informações relacionadas com notificações informativas e de avaliação ([106]).

([98]) De acordo com as informações prestadas pelas autoridades do Reino Unido, durante o período abrangido pelo relatório anual para 2019-2020 do comissário para a informação, não foi detetada qualquer infração em cerca de 25% dos casos, em cerca de 29% dos casos foi pedido ao titular dos dados que comunicasse a preocupação ao responsável pelo tratamento pela primeira vez, que aguardasse pela resposta do responsável pelo tratamento ou que continuasse um diálogo em curso com o responsável pelo tratamento, em cerca de 17% dos casos não foi detetada qualquer infração, mas foi dado um conselho ao responsável pelo tratamento, em cerca de 25% dos casos o comissário para a informação detetou uma infração e deu um conselho ao responsável pelo tratamento ou o responsável pelo tratamento foi obrigado a adotar certas medidas, em cerca de 3% dos casos foi determinado que a reclamação não se enquadrava no Regulamento (UE) 2016/679 e cerca de 1% dos casos foram encaminhados para outra autoridade de proteção de dados no âmbito do Comité Europeu para a Proteção de Dados.

([99]) O ICO pode dar início a essas investigações com base nas informações recebidas de diversas fontes, incluindo notificações sobre violações de dados pessoais, comunicações de outras autoridades públicas do Reino Unido ou de autoridades estrangeiras de proteção de dados e reclamações de pessoas singulares ou organizações da sociedade civil.

([100]) *Information Commissioner's Annual Report and Financial Statements 2019-2020* (ver a nota de rodapé 81).

([101]) De acordo com o relatório anual anterior, que abrange o período de 2018-2019, o comissário para a informação emitiu 22 notificações de sanção ao abrigo do DPA 1998 durante o período de comunicação, sendo que as coimas contabilizaram 3 010 610 GBP, incluindo duas coimas no valor de 500 000 GBP (o valor máximo permitido ao abrigo do DPA 1998). Em 2018, o comissário para a informação investigou a utilização das análises de dados para fins políticos após as revelações sobre a Cambridge Analytica. A investigação resultou num relatório sobre políticas, num conjunto de recomendações, numa coima no valor de 500 000 GBP contra o Facebook e numa notificação de execução dirigida à Aggregate IQ, uma corretora de dados canadiana, a ordenar que a empresa apagasse os dados pessoais dos cidadãos e habitantes do Reino Unido que tinha na sua posse (ver o relatório anual e demonstrações financeiras para 2018-2019 do comissário para a informação, disponível na seguinte ligação https://ico.org.uk/media/about-the-ico/documents/2615262/annual-report-201819.pdf)

([102]) Para obter um resumo das medidas de execução adotadas, consultar o sítio web do ICO, disponível na seguinte ligação: https://ico.org.uk/action-weve-taken/enforcement/

([103]) *Section 170* do DPA 2018.

([104]) *Section 171* do DPA 2018.

([105]) *Section 119* do DPA 2018.

([106]) *Sections 144* e *148* do DPA 2018.

2.6.3 *Supervisão do poder judicial*

(99) A supervisão do tratamento de dados pessoais pelos tribunais e pelo poder judicial tem dois objetivos. Caso o titular de um cargo judicial ou um tribunal não atue no exercício de uma função jurisdicional, o ICO encarrega-se da supervisão. Caso o responsável pelo tratamento atue no exercício de uma função jurisdicional, o ICO não pode exercer as suas funções de supervisão ([107]) e a supervisão é realizada por organismos especiais. Tal reflete a abordagem adotada no Regulamento (UE) 2016/679 (artigo 55.º, n.º 3).

(100) Em particular, no segundo cenário, no caso dos tribunais da Inglaterra e do País de Gales e dos tribunais de primeira instância (*first-tier tribunals*) e superiores (*upper tribunals*) da Inglaterra e do País de Gales, essa supervisão é realizada pelo Painel de Proteção dos Dados Judiciais ([108]). Além disso, o presidente do sistema judiciário (*Lord Chief Justice*) e o presidente dos tribunais (*Senior President of Tribunals*) emitiram uma notificação de privacidade ([109]), que define a forma como os tribunais da Inglaterra e do País de Gales tratam os dados pessoais para uma função judicial. Os sistemas judiciais da Irlanda do Norte ([110]) e da Escócia ([111]) emitiram uma notificação semelhante.

(101) Além disso, na Irlanda do Norte, o presidente do sistema judiciário da Irlanda do Norte nomeou um juiz do *High Court* como juiz supervisor de dados ([112]). Também emitiram orientações dirigidas ao sistema judicial da Irlanda do Norte sobre o que fazer em caso de perda ou potencial perda de dados e como tratar de problemas decorrentes dessa perda ([113]).

(102) Na Escócia, o *Lord President* (Lorde Presidente) nomeou um juiz supervisor de dados para investigar as reclamações associadas a violações da proteção de dados. Isto encontra-se enunciado nas regras em matéria de reclamações judiciais, que refletem as regras estabelecidas para a Inglaterra e o País de Gales ([114]).

(103) Por último, no *Supreme Court* (Supremo Tribunal), um dos juízes do *Supreme Court* é nomeado para supervisionar a proteção de dados.

2.6.4 *Recurso*

(104) A fim de assegurar uma proteção adequada e, nomeadamente, o exercício dos direitos individuais, o titular dos dados deve dispor de vias de recurso administrativas e judiciais eficazes, incluindo a possibilidade de obter uma indemnização por danos.

([107]) *Section 117* do DPA 2018.

([108]) O painel é responsável por fornecer orientações e formação ao poder judicial. Também trata das reclamações efetuadas pelos titulares dos dados no que diz respeito ao tratamento de dados pessoais pelos tribunais e pelas pessoas singulares no exercício de uma função jurisdicional. O painel pretende dar os meios necessários para a resolução de uma reclamação. Se o autor da reclamação estiver insatisfeito com uma decisão do painel, e tiver facultado provas adicionais, este poderá reconsiderar a sua decisão. Embora o painel não imponha sanções financeiras, caso o Painel considere que existe uma violação suficientemente grave do DPA 2018, poderá encaminhar a reclamação para o *Judicial Conduct Investigation Office* (JCIO), que investigará a reclamação. Caso a reclamação seja aceite, cabe ao Lorde Chanceler (*Lord Chancellor*) e ao presidente do sistema judiciário (ou um juiz delegado para atuar em seu nome) decidir qual a medida que deverá ser tomada contra o titular do cargo judicial. As medidas poderão ser, por ordem de gravidade: conselho formal, advertência formal e repreensão e, em última instância, exoneração do cargo. Em caso de insatisfação com a forma como a reclamação foi investigada pelo JCIO, uma pessoa singular poderá efetuar nova reclamação junto do provedor para as nomeações e as condutas judiciais (ver https://www.gov.uk/government/organisations/judicial-appointments-and-conduct--ombudsman). O provedor dispõe de poderes para solicitar ao JCIO que investigue novamente uma reclamação e pode propor que o autor da reclamação receba uma indemnização, caso tenha motivos para acreditar que este sofreu danos resultantes da administração desadequada.

([109]) A notificação de privacidade emitida pelo presidente do sistema judiciário e o presidente dos tribunais pode ser consultada na seguinte ligação: https://www.judiciary.uk/about-the-judiciary/judiciary-and-data-protection-privacy-notice

([110]) A notificação de privacidade emitida pelo presidente do sistema judiciário da Irlanda do Norte pode ser consultada na seguinte ligação: https://judiciaryni.uk/data-privacy

([111]) A notificação de privacidade emitida pelos tribunais escoceses está disponível na seguinte ligação: https://www.judiciary.uk/about--the-judiciary/judiciary-and-data-protection-privacy-notice

([112]) O juiz supervisor de dados emite orientações dirigidas ao sistema judicial e investiga violações e/ou reclamações relativas ao tratamento de dados pessoais efetuado pelos tribunais ou por pessoas singulares no exercício da sua função jurisdicional.

([113]) Caso a reclamação ou a violação seja considerada grave, a mesma é encaminhada para o responsável das reclamações judiciais para continuar a ser investigada, de acordo com o *Code of Practice on Complaints* (código de boas práticas sobre reclamações) do presidente do sistema judiciário da Irlanda do Norte. O resultado dessa reclamação pode incluir: a ausência de medidas adicionais, aconselhamento, formação ou mentoria, advertência informal, advertência formal, advertência final, restrição da prática ou encaminhamento para um tribunal. O *Code of Practice on Complaints*, emitido pelo presidente do sistema judiciário da Irlanda do Norte, está disponível na seguinte ligação:https://judiciaryni.uk/sites/judiciary/files/media-files/14G.%20CODE%20OF%20PRACTICE%20Judicial%20~%2028%20Feb%2013%20%28Final%29%20updated%20with%20new%20comp..__1.pdf

([114]) Todas as reclamações efetuadas são investigadas pelo juiz supervisor de dados e encaminhadas para o *Lord President*, que dispõe de poderes para emitir pareceres, advertências formais ou repreensões caso considere necessário (existem regras equivalentes para membros do tribunal, que se encontram disponíveis na seguinte ligação: https://www.judiciary.scot/docs/librariesprovider3/judiciarydocuments/complaints/complaintsaboutthejudiciaryscotlandrules2017_1d392ab6e14f6425aa0c7f48d062f5cc5.pdf?sfvrsn=5d3eb9a1_2)

(105) Em primeiro lugar, um titular dos dados tem o direito de apresentar reclamação ao comissário para a informação caso considere que existe uma violação do RGPD do Reino Unido no que diz respeito aos seus dados pessoais ([115]). O RGPD do Reino Unido mantém as regras previstas no artigo 77.º do Regulamento (UE) 2016/679 relativas a esse direito sem efetuar alterações significativas. O mesmo se aplica ao artigo 57.º, n.º 1, alínea f), e n.º 2, que enumera as atribuições do comissário relativas ao tratamento de reclamações. Conforme descrito nos considerandos 92 a 98 acima, o comissário para a informação tem o poder de avaliar o cumprimento do RGPD do Reino Unido e do DPA 2018 do responsável pelo tratamento e do subcontratante, de exigir que estes tomem ou se abstenham de tomar as medidas necessárias em caso de incumprimento e de impor coimas.

(106) Em segundo lugar, o RGPD do Reino Unido e o DPA 2018 preveem o direito à ação judicial contra o comissário para a informação. Nos termos do artigo 78.º, n.º 1, do RGPD do Reino Unido, as pessoas singulares têm direito à ação judicial contra as decisões juridicamente vinculativas do comissário que lhes digam respeito. No contexto do controlo jurisdicional, o juiz examina a decisão que está a ser contestada no processo e decide se o comissário para a informação atuou licitamente. Além disso, nos termos do artigo 78.º, n.º 2, do RGPD do Reino Unido, caso o comissário não trate adequadamente uma reclamação efetuada pelo titular de dados, ([116]) o autor da reclamação tem direito à ação judicial. O autor da reclamação pode recorrer a um tribunal de primeira instância para ordenar que o comissário adote as medidas adequadas para dar uma resposta à reclamação ou para informar o autor da reclamação sobre o andamento da mesma ([117]). Além disso, qualquer pessoa que receba uma das notificações supramencionadas (notificações informativas, de avaliação, de execução ou de sanção) emitidas pelo comissário pode recorrer a um tribunal de primeira instância ([118]). Se o tribunal considerar que a decisão do comissário não está de acordo com a lei ou que o comissário para a informação deveria ter exercido o seu critério de outra forma, o tribunal deve permitir o recurso ou substituir outra notificação ou decisão que poderia ter sido emitida ou dada pelo comissário para a informação.

(107) Em terceiro lugar, as pessoas singulares podem obter direito ao recurso judicial contra um responsável pelo tratamento ou um subcontratante diretamente nos tribunais, ao abrigo do artigo 79.º do RGPD do Reino Unido e da *section 167* do DPA 2018. No caso de uma ação intentada por um titular de dados, se um tribunal decidir que houve uma violação dos direitos do titular dos dados ao abrigo da legislação em matéria de proteção de dados, o tribunal pode ordenar que o responsável pelo tratamento ou um subcontratante que atue em nome dele tome as medidas especificadas na ordem ou se abstenha de tomar as medidas especificadas na ordem, no que diz respeito ao tratamento.

(108) Além disso, nos termos do artigo 82.º do RGPD do Reino Unido e da *section 168* do DPA 2018, qualquer pessoa que tenha sofrido danos materiais ou imateriais devido a uma violação do RGPD do Reino Unido tem direito a receber uma indemnização do responsável pelo tratamento ou do subcontratante pelos danos sofridos. As regras relativas à indemnização e à responsabilidade previstas no artigo 82.º, n.ºs 1 a 5, do RGPD do Reino Unido são idênticas às regras correspondentes do Regulamento (UE) 2016/679. Ao abrigo da *section 168* do DPA 2018, os danos imateriais incluem sofrimento emocional. Nos termos do artigo 80.º do RGPD do Reino Unido, o titular dos dados tem o direito de mandatar um organismo ou organização representante para, em seu nome, apresentar reclamação junto do comissário (nos termos do artigo 77.º do RGPD do Reino Unido) e exercer os direitos a que se referem os artigos 78.º (direito à ação judicial contra o comissário), 79.º (direito à ação judicial contra um responsável pelo tratamento ou um subcontratante) e 82.º (direito de indemnização e responsabilidade) do RGPD do Reino Unido.

(109) Em quarto lugar, e para além das vias de recurso descritas acima, qualquer pessoa que considere que houve uma violação dos seus direitos, nomeadamente do direito à privacidade e à proteção dos dados, por parte das autoridades públicas, pode obter reparação junto dos tribunais do Reino Unido, ao abrigo do *Human Rights Act 1998* ([119]). Qualquer pessoa que afirme que uma autoridade pública atuou (ou pretende atuar) de uma forma incompatível com um dos direitos da Convenção e, consequentemente, ilícita, nos termos da *section 6(1)* do *Human Rights Act 1998*, pode intentar uma ação junto do tribunal competente contra a autoridade em questão ou recorrer a processos judiciais para fazer valer os seus direitos, sempre que essa pessoa seja (ou venha a ser) vítima de uma ação ilícita.

(110) Se o tribunal considerar que alguma das ações de uma autoridade pública foi ilícita, pode decretar essa medida ou recurso ou efetuar essa ordem, dentro dos seus poderes e de uma forma que considere justa e adequada ([120]). O tribunal pode igualmente constatar que uma das disposições do direito primário é incompatível com um direito da Convenção.

([115]) Artigo 77.º do RGPD do Reino Unido.

([116]) A *section 166* do DPA 2018 diz respeito especificamente às seguintes situações: a) o comissário não toma as medidas adequadas para dar resposta à reclamação, b) o comissário não informa o autor da reclamação do andamento ou do resultado da reclamação antes do final do prazo de três meses que tem início quando o comissário recebeu a reclamação ou c) se a análise da reclamação efetuada pelo comissário não for concluída dentro desse prazo e se o comissário não fornecer essas informações ao autor da reclamação num prazo subsequente de três meses.

([117]) Artigo 78.º, n.º 2, do RGPD do Reino Unido e *section 166* do DPA 2018.

([118]) Artigo 78.º, n.º 1, do RGPD do Reino Unido e *section 162* do DPA 2018.

([119]) *Section 7(1)* do *Human Rights Act 1998*. De acordo com a *section 7(7)*, uma pessoa é vítima de uma ação ilícita apenas se puder ser considerada vítima para efeitos do artigo 34.º da Convenção Europeia dos Direitos Humanos, caso as ações sejam intentadas junto do Tribunal Europeu dos Direitos Humanos em relação a essa ação.

([120]) *Section 8(1)* do *Human Rights Act 1998*.

(111) Por último, depois de esgotarem as vias de recurso nacionais, as pessoas singulares podem obter junto do Tribunal Europeu dos Direitos Humanos por violações dos direitos garantidos pela Convenção Europeia dos Direitos Humanos.

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

(112) A Comissão avaliou igualmente o quadro jurídico implementado pelo Reino Unido para a recolha e a utilização subsequente de dados pessoais transferidos por autoridades públicas do Reino Unido para operadores comerciais no Reino Unido, para fins de interesse público, designadamente para efeitos de aplicação do direito penal e de segurança nacional (a seguir designado por «acesso governamental»). Ao avaliar se as condições em que o governo acede aos dados transferidos para o Reino Unido ao abrigo da presente decisão cumpririam o teste de «equivalência essencial» nos termos do artigo 45.º, n.º 1, do Regulamento (UE) 2016/679, conforme interpretado pelo Tribunal de Justiça da União Europeia, à luz da Carta dos Direitos Fundamentais, a Comissão teve em conta sobretudo os seguintes critérios.

(113) Em primeiro lugar, qualquer restrição ao direito de proteção de dados pessoais deve ser prevista por lei, o que implica que a própria base jurídica que permite a ingerência nesses direitos deve definir o alcance da restrição ao exercício do direito em causa ([121]).

(114) Em segundo lugar, para satisfazer o requisito da proporcionalidade segundo o qual as derrogações à proteção de dados pessoais e as suas restrições devem ocorrer na estrita medida do necessário numa sociedade democrática para alcançar os objetivos específicos de interesse geral equivalentes aos reconhecidos pela União, a regulamentação do país terceiro em causa que permite a ingerência deve prever regras claras e precisas que regulem o alcance e a aplicação das medidas em causa e imponham requisitos mínimos, de modo que as pessoas cujos dados foram transferidos disponham de garantias suficientes que permitam proteger eficazmente os seus dados pessoais contra os riscos de abuso ([122]). A regulamentação deve, em especial, indicar em que circunstâncias e em que condições se pode adotar uma medida que preveja o tratamento desses dados ([123]), bem como sujeitar o cumprimento desses requisitos a uma supervisão independente ([124]).

(115) Em terceiro lugar, essa regulamentação deve ser juridicamente vinculativa ao abrigo da legislação interna e estes requisitos legais devem não só ser vinculativos para as autoridades, mas também executáveis junto dos tribunais contra as autoridades do país terceiro em questão ([125]). Em particular, os titulares de dados devem dispor da possibilidade de recorrer a medidas jurídicas corretivas eficazes num tribunal independente e imparcial, para ter acesso a dados pessoais que lhes digam respeito ou para obter a retificação ou a supressão desses dados ([126]).

3.1 **Quadro jurídico geral**

(116) Enquanto exercício de poder de uma autoridade pública, o acesso governamental no Reino Unido deve ter lugar no pleno respeito pela lei. O Reino Unido ratificou a Convenção Europeia dos Direitos Humanos (ver o considerando 9) e todas as autoridades públicas do Reino Unido são obrigadas a cumprir a Convenção ([127]). O artigo 8.º da Convenção prevê que não pode haver ingerência senão quando esta ingerência estiver prevista na lei, tendo em conta os interesses de um dos objetivos estabelecidos no artigo 8.º, n.º 2, e proporcionais à luz desse objetivo. O artigo 8.º também exige que a ingerência seja «previsível», ou seja, que tenha uma base clara e acessível prevista na lei e que a lei contenha garantias adequadas para evitar abusos.

(117) Além disso, na sua jurisprudência, o Tribunal Europeu dos Direitos Humanos especificou que qualquer ingerência no direito à privacidade e à proteção dos dados deve ser sujeita a um sistema de supervisão eficaz, independente e imparcial que deve ser fornecido por um juiz ou por outro organismo independente ([128]) (por exemplo, uma autoridade administrativa ou um órgão parlamentar).

([121]) Ver *Schrems II*, n.ºs 174 a 175, e a jurisprudência referida. Ver ainda, no que diz respeito ao acesso das autoridades públicas dos Estados-Membros, processo C-623/17, *Privacy International*, ECLI:EU:C:2020:790, n.º 65; e Processos apensos C-511/18, C-512/18 e C-520/18 *La Quadrature du Net e o*. ECLI:EU:C:2020:791, n.º 175.

([122]) Ver *Schrems II*, n.ºs 176 e 181, bem como a jurisprudência referida. Ver ainda, no que diz respeito ao acesso das autoridades públicas dos Estados-Membros, *Privacy International*, n.º 68; e *La Quadrature du Net e o*., n.º 132.

([123]) Ver *Schrems II*, n.º 176. Ver ainda, no que diz respeito ao acesso das autoridades públicas dos Estados-Membros, *Privacy International*, n.º 68; e *La Quadrature du Net e o*., n.º 132.

([124]) Ver *Schrems II*, n.º 179.

([125]) Ver *Schrems II*, n.ºs 181 a 182.

([126]) Ver *Schrems I*, n.º 95, e *Schrems II*, n.º 194. A esse respeito, o TJUE salientou que a observância do artigo 47.º da Carta dos Direitos Fundamentais, que garante o direito à ação por um tribunal independente e imparcial, «faz parte do nível de proteção exigido na União [e] deve ser constatada pela Comissão antes de adotar uma decisão de adequação ao abrigo do artigo 45.º, n.º 1, do Regulamento (UE) 2016/679» (*Schrems II*, n.º 186).

([127]) *Section 6* do *Human Rights Act 1998*.

([128]) Tribunal Europeu dos Direitos Humanos, *Klass e o./Alemanha*, processo n.º 5029/71, n.ºs 17 a 51.

(118) Além disso, as pessoas singulares devem ter direito a uma ação e o Tribunal Europeu dos Direitos Humanos esclareceu que a ação deve ser proporcionada por um organismo independente e imparcial que adotou o seu próprio regulamento interno, composto por membros que têm ou tiveram um cargo judicial elevado ou são advogados experientes e que não deve haver encargos evidentes a superar para intentar uma ação. No âmbito da apreciação de reclamações apresentadas por pessoas singulares, o órgão independente e imparcial deve ter acesso a todas as informações pertinentes, incluindo elementos confidenciais. Por último, deve ter poderes para impor a correção do incumprimento ([129]).

(119) O Reino Unido também ratificou a Convenção do Conselho da Europa para a Proteção das Pessoas Relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal (convenção 108) e assinou o Protocolo que altera a Convenção para a Proteção das Pessoas Relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal (conhecida como Convenção 108+) em 2018 ([130]). O artigo 9.º da Convenção 108 prevê que as derrogações dos princípios gerais de proteção de dados (artigo 5.º Qualidade dos dados), das normas que regem as categorias especiais de dados (artigo 6.º — Categorias especiais de dados) e dos direitos dos titulares dos dados (artigo 8.º — Garantias suplementares aplicáveis ao titular dos dados) apenas são permitidas quando essa derrogação está prevista na lei da Parte e constitui uma medida necessária numa sociedade democrática à proteção da segurança do Estado, da segurança pública, dos interesses monetários do Estado ou da repressão de infrações penais ou à proteção do titular dos dados ou dos direitos e liberdades de outrem ([131]).

(120) Como tal, através da adesão ao Conselho da Europa, da adesão à Convenção Europeia dos Direitos Humanos e da submissão à jurisdição do Tribunal Europeu dos Direitos Humanos, o Reino Unido está sujeito a um conjunto de obrigações, consagradas no direito internacional, o que implica que o seu sistema de acesso governamental deve respeitar princípios, garantias e direitos individuais semelhantes aos garantidos ao abrigo do direito da UE e aplicáveis aos Estados-Membros. Conforme salienta o considerando 19, a adesão contínua a esses instrumentos é, como tal, um elemento particularmente importante da avaliação na qual esta decisão se baseia.

(121) Além disso, o DPA 2018 garante salvaguardas e direitos específicos em matéria de proteção de dados nos casos em que os dados são tratados por autoridades públicas, incluindo por organismos de aplicação da lei e de segurança nacional.

(122) Em particular, a parte 3 do DPA 2018 define o regime para o tratamento de dados pessoais no contexto da aplicação do direito penal, que foi adotado para transpor a Diretiva (UE) 2016/680. A parte 3 do DPA 2018 é aplicável 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 ([132]).

(123) A *section 30* do DPA define o conceito de «autoridade competente» como uma das pessoas constantes do *schedule 7* do DPA 2018, bem como qualquer outra pessoa desde que desempenhe funções legais para efeitos de aplicação da lei ([133]). Conforme explicado abaixo (ver o considerando 139), determinadas autoridades competentes (por exemplo, a *National Crime Agency* [agência britânica de combate à criminalidade]) podem utilizar, em determinadas condições, os poderes previstos no *Investigatory Power Act* [Lei de 2016 relativa aos poderes de investigação] (IPA 2016). Neste caso, as garantias previstas no IPA 2016 serão aplicáveis para além das previstas na parte 3 do DPA 2018. Os serviços de informações (o *Secret Intelligence Service*, o *Security Service* e o quartel-general de comunicações do governo) não são «autoridades competentes» ([134]) o âmbito da parte 3 do DPA 2018 e, por conseguinte, as regras aí previstas não são aplicáveis a nenhuma das suas atividades. É dedicada uma parte específica do DPA 2018 (parte 4) ao tratamento de dados pessoais pelos serviços de informações (para mais pormenores, ver o considerando 125).

([129]) Tribunal Europeu dos Direitos Humanos, *Kennedy/Reino Unido*, processo n.º 26839/05, («Kennedy»), n.ºs 167 e 190.

([130]) Para obter mais informações sobre a Convenção Europeia dos Direitos Humanos e a sua integração no direito do Reino Unido através do *Human Rights Act 1998*, bem como na Convenção 108, ver o considerando 9 acima.

([131]) De igual forma, nos termos do artigo 11.º da Convenção 108+, as restrições de determinados direitos e obrigações específicos da Convenção para efeitos de segurança nacional ou de prevenção, investigação e repressão de infrações penais e da execução de sanções penais apenas são permitidas quando tal restrição está prevista por lei, respeita a essência dos direitos e liberdades fundamentais e constitui uma medida necessária e proporcionada numa sociedade democrática. As atividades de tratamento para efeitos de segurança nacional e defesa também devem estar sujeitas a uma análise e supervisão eficazes e independentes ao abrigo da legislação interna da respetiva Parte da Convenção

([132]) *Section 31* do DPA 2018.

([133]) As autoridades competentes constantes do *schedule 7* incluem não só forças policiais, mas também todos os ministérios do Governo do Reino Unido, bem como outras autoridades com funções de investigação [por exemplo, o Comissário para o *Her Majesty's Revenue and Customs* (serviço real de fiscalidade e alfândegas do Reino Unido), a *National Crime Agency*, a *Welsh Revenue Authority* (autoridade fiscal do País de Gales), a *Competition and Markets Authority* (autoridade para a concorrência e os mercados) ou o *Her Majesty's Land Register* (registo predial)], agências de ação penal, outras agências de justiça penal e outros titulares ou organizações que realizam atividades de aplicação da lei (entre esses, o *schedule 7* do DPA 2018 enuncia os diretores do Ministério Público, o diretor do Ministério Público da Irlanda do Norte e o comissário para a informação).

([134]) *Section 30(2)* do DPA 2018.

(124) À semelhança da Diretiva (UE) 2016/680, a parte 3 do DPA 2018 estabelece os princípios de licitude e lealdade ([135]), limitação das finalidades ([136]), minimização dos dados ([137]), exatidão ([138]), limitação da conservação ([139]) e segurança ([140]). A legislação impõe obrigações de transparência específicas ([141]) e prevê o direito de acesso ([142]), retificação e apagamento ([143]) e o direito de não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado ([144]) conferidos às pessoas singulares. A autoridades competentes são igualmente obrigadas a aplicar a proteção de dados desde a conceção e por defeito, a conservar registos das atividades de tratamento e, no caso de determinadas operações de tratamento, a realizar avaliações do impacto sobre a proteção de dados e a efetuar uma consulta prévia do comissário para a informação ([145]). Nos termos da *section 56* do DPA 2018, são obrigadas a comprovar o cumprimento. Além disso, são obrigadas a aplicar medidas adequadas para garantir a segurança do tratamento ([146]) e estão sujeitas a obrigações específicas em caso de violação dos dados, incluindo notificações dessas violações ao comissário para a informação e aos titulares dos dados ([147]). À semelhança do que acontece na Diretiva (UE) 2016/680, existe igualmente a obrigação de o responsável pelo tratamento (a menos que seja um tribunal ou outra autoridade judicial no exercício da sua função jurisdicional) designar um encarregado da proteção de dados (EPD) ([148]) que preste assistência ao responsável pelo tratamento no sentido de assegurar o cumprimento das suas obrigações, bem como de controlar esse cumprimento ([149]). Além disso, a legislação impõe requisitos específicos para transferências internacionais de dados pessoais para países terceiros ou organizações internacionais para efeitos de aplicação da lei, de modo a garantir a continuidade da proteção ([150]). Na mesma data da presente decisão, a Comissão adotou uma decisão de adequação 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 assegura um nível de proteção essencialmente equivalente ao assegurado na Diretiva (UE) 2016/680.

(125) A parte 4 do DPA 2018 é aplicável a qualquer tratamento efetuado por ou em nome dos serviços de informações. Em particular, estabelece os principais princípios de proteção de dados (licitude, lealdade e transparência ([151]); limitação das finalidades ([152]); minimização dos dados ([153]); exatidão ([154]); limitação da conservação ([155]) e segurança ([156])), impõe condições para o tratamento de categorias especiais de dados ([157]), prevê os direitos dos titulares dos dados ([158]), exige a

([135]) *Section 35* do DPA 2018.
([136]) *Section 36* do DPA 2018.
([137]) *Section 37* do DPA 2018.
([138]) *Section 38* do DPA 2018.
([139]) *Section 39* do DPA 2018.
([140]) *Section 40* do DPA 2018.
([141]) *Section 44* do DPA 2018.
([142]) *Section 45* do DPA 2018.
([143]) *Sections 46* e *47* do DPA 2018.
([144]) *Sections 49* e *50* do DPA 2018.
([145]) *Sections 56* a *65* do DPA 2018.
([146]) *Section 66* do DPA 2018.
([147]) *Sections 67* e *68* do DPA 2018.
([148]) *Sections 69* a *71* do DPA 2018.
([149]) *Sections 67* e *68* do DPA 2018.
([150]) Parte 3, capítulo 5, do DPA 2018.
([151]) Ao abrigo da *section 86(6)* do DPA 2018, para determinar a lealdade e a transparência do tratamento, o método para a sua obtenção deve ser tido em consideração. Neste sentido, o requisito de lealdade e transparência é conseguido se os dados forem obtidos de uma pessoa que tenha uma autorização lícita ou que seja obrigada a fornecê-los.
([152]) Ao abrigo da *section 87* do DPA 2018, as finalidades do tratamento devem ser determinadas, explícitas e legítimas. Os dados não devem ser tratados de uma forma incompatível com as finalidades para as quais foram recolhidos. Ao abrigo da *section 87(3)* do DPA 2018, só pode ser permitido um tratamento de dados pessoais compatível se o responsável pelo tratamento estiver autorizado por lei a tratar os dados para essa finalidade e o tratamento for necessário e proporcional a essa outra finalidade. As operações de tratamento para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos, deverão ser consideradas tratamento compatível e estão sujeitas a garantias adequadas [*section 87(4)* do DPA 2018].
([153]) Os dados pessoais devem ser adequados, relevantes e não excessivos (*section 88* do DPA 2018).
([154]) Os dados pessoais devem ser precisos e atualizados (*section 89* do DPA 2018).
([155]) Os dados pessoais devem ser conservados apenas durante o período necessário (*section 90* do DPA 2018).
([156]) O sexto princípio de proteção de dados é que os dados pessoais devem ser tratados de uma forma que inclua a tomada de medidas de segurança adequadas no que diz respeito aos riscos decorrentes do tratamento de dados pessoais. Os riscos incluem (entre outros) acesso acidental ou não autorizado aos dados pessoais ou a respetiva destruição, perda, utilização, modificação ou divulgação (*section 91* do DPA 2018). A *section 107* exige igualmente que 1) cada responsável pelo tratamento aplique as medidas de segurança adequadas para atenuar os riscos decorrentes do tratamento de dados pessoais e 2) em caso de tratamento automatizado, cada responsável pelo tratamento e subcontratante aplique medidas preventivas ou de atenuação com base numa avaliação do risco.
([157]) *Section 86(2)(b)* e *schedule 10* do DPA 2018.
([158]) Parte 4, capítulo 3, do DPA 2018, nomeadamente os direitos: de acesso, de retificação e apagamento, de se opor ao tratamento e de não ficar sujeito a nenhuma decisão tomada exclusivamente com base no tratamento automatizado, de intervir numa decisão tomada com base no tratamento automatizado e de ser informado de uma decisão tomada com base no tratamento automatizado. Além disso, o responsável pelo tratamento deve informar o titular dos dados do tratamento dos seus dados pessoais. Conforme explicado nas orientações do ICO sobre o tratamento efetuado pelos serviços de informações, as pessoas singulares podem exercer todos os seus direitos (incluindo um pedido de retificação) ao apresentar reclamação ao ICO ou interpondo uma ação em tribunal (ver as orientações do ICO para o tratamento efetuado pelos serviços de informações, disponível na seguinte ligação: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-intelligence-services-processing/).

proteção de dados desde a conceção ([159]) e regula as transferências internacionais de dados pessoais ([160]). O ICO emitiu recentemente orientações pormenorizadas sobre o tratamento efetuado pelas agências de informações ao abrigo da parte 4 do DPA 2018 ([161]).

(126) Paralelamente, a *section 110* do DPA 2018 prevê uma isenção das disposições determinadas na parte 4 ([162]) do DPA 2018 quando essa isenção é necessária para proteger a segurança nacional. É possível recorrer a esta isenção com base numa análise casuística ([163]). Conforme explicado pelas autoridades do Reino Unido e confirmado pela jurisprudência, um «responsável pelo tratamento deve ter em conta as consequências efetivas para a segurança nacional ou a defesa caso tenha de cumprir a disposição específica em matéria de proteção de dados e se consegue cumprir razoavelmente a regra habitual sem afetar a segurança nacional ou a defesa» ([164]). Cabe à supervisão do ICO determinar se a isenção foi usada adequadamente ou não ([165]).

(127) Além disso, no que se refere à possibilidade de restringir a aplicação das disposições acima referidas, de acordo com a *section 111* do DPA 2018, para efeitos de proteção da «segurança nacional», um responsável pelo tratamento pode solicitar um certificado assinado por um ministro do Gabinete ou pelo procurador-geral (*Attorney General*) que ateste que a restrição desses direitos constitui uma medida necessária e proporcionada para a proteção da segurança nacional ([166]).

(128) O governo do Reino Unido emitiu orientações para auxiliar os responsáveis pelo tratamento a decidir se devem solicitar um certificado de segurança nacional ao abrigo do DPA 2018, que saliente que a restrição dos direitos dos titulares dos dados para efeitos de proteção da segurança nacional é uma medida necessária e proporcionada ([167]). Todos os certificados de segurança nacional terão de ser publicados no sítio Web do ICO ([168]).

([159]) *Section 103* do DPA 2018.

([160]) *Section 109* do DPA 2018. É possível efetuar transferências de dados pessoais para organizações internacionais ou países fora do Reino Unido caso estas constituam uma medida necessária e proporcionada para efeitos das funções legais do responsável pelo tratamento ou para outras finalidades previstas em secções específicas do *Security Service Act 1989* (Lei de 1989 relativa ao Serviço de Segurança) e do *Intelligence Services Act 1994*.

([161]) Orientações do ICO, ver a nota de rodapé 158.
Section 30 do DPA 2018 e *schedule 7* do DPA 2018.

([162]) A *section 110(2)* do DPA 2018 enumera as disposições em que é permitida uma isenção. Inclui os princípios de proteção de dados (à exceção do princípio da licitude), os direitos dos titulares dos dados, a obrigação de informar o comissário para a informação sobre uma violação de dados, os poderes de inspeção do comissário para a informação de acordo com as obrigações internacionais, os poderes de execução do comissário para a informação, as disposições que tornam determinadas violações da proteção de dados uma infração penal e as disposições relativas a fins de tratamento especiais, como fins jornalísticos e fins de expressão académica ou artística.

([163]) Ver *Baker/Secretary of State*, ver a nota de rodapé 61.

([164]) *Explanatory Framework for Adequacy Discussions, section H: National Security Data Protection and Investigatory Powers Framework*, p. 15 a 16 (ver a nota de rodapé 31). Ver ainda *Baker/Secretary of State* (ver a nota de rodapé 61), no qual o tribunal anulou um certificado de segurança nacional emitido pelo ministro da Administração Interna e que confirma a aplicação da isenção de segurança nacional, tendo em conta que não havia motivo para criar uma isenção geral da obrigação de responder a pedidos de acesso e que, permitir essa isenção em todas as circunstâncias sem uma análise casuística, excedeu o que seria necessário e proporcionado para a proteção da segurança nacional.

([165]) Ver o memorando de entendimento entre o ICO e a UKIC, segundo o qual «[a]pós a receção de uma reclamação efetuada por um titular de dados, o ICO certificar-se-á de que a questão foi tratada corretamente e, se for caso disso, que a aplicação de eventuais isenções foi utilizada adequadamente». Memorando de entendimento entre o Gabinete do Comissário para a Informação e o *UK Intelligence Community* (comunidade dos serviços de informações do Reino Unido), ponto 16, disponível na seguinte ligação: https://ico.org.uk/media/about-the-ico/mou/2617438/uk-intelligence-community-ico-mou.pdf

([166]) O DPA 2018 revogou a possibilidade de emitir certificados ao abrigo da *section 28(2)* da *Data Protection Act 1998*. Todavia, continua a existir a possibilidade de emitir «certificados antigos», na medida em que existe um desafio histórico ao abrigo da lei de 1998 (ver n.º 17 da parte 5 do *schedule 20* do DPA 2018). Todavia, esta possibilidade parece ser muito rara e só se aplicará em casos limitados, como, por exemplo, quando um titular dos dados contesta a utilização da isenção relativa à segurança nacional a respeito de um tratamento efetuado ao abrigo da lei de 1998 por uma autoridade pública. Importa notar que, nestes casos, a *section 28* do DPA 1998 será aplicável na sua totalidade, incluindo, por conseguinte, a possibilidade de o titular dos dados contestar o certificado perante o tribunal.

([167]) Orientações do Governo do Reino Unido em matéria de certificados de segurança nacional ao abrigo do *Data Protection Act 2018*, disponível na seguinte ligação: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/910279/Data_Protection_Act_2018_-_National_Security_Certificates_Guidance.pdf. De acordo com a explicação dada pelas autoridades do Reino Unido, embora um certificado seja uma prova conclusiva de que, no que diz respeito aos dados ou ao tratamento descrito no certificado, se aplica a isenção, este não exclui a obrigação de o responsável pelo tratamento realizar uma análise casuística para avaliar a necessidade de recorrer à isenção.

([168]) De acordo com a *section 130* do DPA 2018, o ICO pode decidir não publicar o texto ou parte do texto do certificado, se tal for contrário ao interesse da segurança nacional ou ao interesse público, ou for suscetível de comprometer a segurança de qualquer pessoa. Nestes casos, o ICO publicará, todavia, o facto de o certificado ter sido emitido.

(129) O certificado deverá ter uma duração fixa não superior a cinco anos, de forma a ser analisado regularmente pelo executivo ([169]). Um certificado deve identificar os dados pessoais ou as categorias de dados pessoais sujeitas à isenção, bem como as disposições do DPA 2018 às quais se aplica a isenção ([170]).

(130) Importa notar que os certificados de segurança nacional não preveem um motivo adicional a fim de restringir os direitos em matéria de proteção de dados por razões de segurança nacional. Por outras palavras, o responsável pelo tratamento ou o subcontratante só pode recorrer a um certificado quando tiver a certeza de que o recurso à isenção de segurança nacional constitui uma medida necessária, sendo que, para isso, tal como explicado acima, deve ser realizada uma análise casuística ([171]). Mesmo que um certificado de segurança nacional se aplique à matéria em questão, o ICO pode investigar se o recurso à isenção de segurança nacional constituía uma medida justificada num caso específico ([172]).

(131) Uma pessoa diretamente afetada pela emissão do certificado pode recorrer ao *Upper Tribunal* ([173]) para contestar o certificado ([174]) ou, caso o certificado inclua a identificação dos dados por meio de uma descrição geral, para contestar a aplicação do mesmo a dados específicos ([175]). O tribunal irá analisar a decisão de emitir um certificado e decidirá se existiram motivos razoáveis para a emissão do certificado ([176]). O tribunal pode ter em conta um vasto conjunto de questões, nomeadamente a necessidade, a proporcionalidade e a licitude, tendo em conta o impacto nos direitos dos titulares de dados e equilibrando a necessidade de proteger a segurança nacional. Consequentemente, o tribunal pode determinar que o certificado não se aplica aos dados pessoais específicos que são o objeto do recurso ([177]).

(132) Ao abrigo do *schedule 11* do DPA 2018, aplica-se um conjunto diferente de possíveis restrições a determinadas disposições da parte 4 do DPA 2018 ([178]) para salvaguardar outros importantes objetivos de interesse público geral ou interesses protegidos, como, por exemplo, privilégio parlamentar, privilégio profissional legal, a conduta dos processos judiciais ou a eficácia do combate das forças armadas ([179]). A aplicação destas disposições está isenta para determinadas categorias de dados («com base na categoria») ou isenta na medida em que a aplicação destas disposições seria suscetível de prejudicar o interesse protegido («com base no prejuízo») ([180]). As isenções com base no prejuízo só podem ser invocadas na medida em que a aplicação das disposições enumeradas em matéria de

([169]) Orientações do Governo do Reino Unido em matéria de certificados de segurança nacional, n.º 15, ver a nota de rodapé 167.

([170]) Orientações do Governo do Reino Unido em matéria de certificados de segurança nacional, n.º 5, ver a nota de rodapé 167.

([171]) Ver a nota de rodapé 164.

([172]) A *section 102* do DPA 2018 exige que o responsável pelo tratamento demonstre que cumpriu o DPA 2018. Para tal, um serviço de informações precisaria de demonstrar ao ICO que, ao recorrer à isenção, teve em conta as circunstâncias específicas do caso. O ICO também publica um registo dos certificados de segurança nacional, que se encontra disponível na seguinte ligação: https://ico.org.uk//about-the-ico/our-information/national-security-certificates/

([173]) O *Upper Tribunal* é o tribunal competente para apreciar os recursos contra as decisões tomadas pelos tribunais administrativos inferiores e dispõe de competências específicas para lidar com recursos diretos contra decisões tomadas por determinados organismos governamentais.

([174]) *Section 111(3)* do DPA 2018.

([175]) *Section 111(5)* do DPA 2018.

([176]) Em *Baker/Secretary of State* (ver a nota de rodapé 61), o *Information Tribunal* anulou um certificado de segurança nacional emitido pelo ministro da Administração Interna, tendo em conta que não havia motivo para criar uma exceção geral da obrigação de responder a pedidos de acesso e que, permitir essa exceção em todas as circunstâncias sem uma análise casuística, excedeu o que seria necessário e proporcionado para a proteção da segurança nacional.

([177]) Orientações do Governo do Reino Unido em matéria de certificados de segurança nacional, n.º 25, ver a nota de rodapé 167.

([178]) Tal inclui: i) os princípios de proteção de dados estabelecidos na parte 4, à exceção do requisito da licitude do tratamento previsto no primeiro princípio e a obrigatoriedade de o tratamento cumprir uma das condições relevantes estabelecidas nos *schedules 9* e *10*; ii) os direitos dos titulares dos dados; e iii) os deveres relativos à denúncia de violações ao ICO.

([179]) A parte 4 do DPA 2018 estabelece o quadro jurídico aplicável a todos os tipos de tratamento de dados pessoais efetuado pelos serviços de informações (e não apenas ao exercício das suas funções de segurança nacional). Por conseguinte, a parte 4 é igualmente aplicável quando as agências de informações tratam dados, por exemplo, para efeitos de gestão de recursos humanos, no contexto de litígios ou de contratos públicos. As restrições enunciadas no *schedule 11* destinam-se principalmente a ser aplicadas nestes outros contextos. Por exemplo, no contexto de um litígio com um trabalhador, pode ser invocada a restrição para efeitos de «processos judiciais» ou, no contexto de contratos públicos, pode ser invocada a restrição para efeitos de «negociação», etc. Tal reflete-se nas orientações do ICO sobre o tratamento efetuado pelos serviços de informações, que menciona a negociação de um acordo entre um serviço de informações e um antigo trabalhador que prossegue um crédito de emprego como exemplo para a aplicação das restrições do *schedule 11* (ver a nota de rodapé 161). Importa igualmente notar que as mesmas restrições estão disponíveis para outras autoridades públicas nos termos do *schedule 2*, parte 2, do DPA 2018.

([180]) De acordo com o *Explanatory Framework* do Reino Unido, as isenções que são «baseadas na categoria» são: i) informações sobre as honras e as dignidades da Coroa que são conferidas; ii) privilégio profissional legal; iii) referências contratuais, de formação ou de educação confidenciais; e iv) guiões e marcas de exames. As isenções «com base no prejuízo» dizem respeito às seguintes questões: i) prevenção ou deteção de crimes; detenção e repressão de infratores; ii) privilégio parlamentar; iii) processos judiciais; iv) a eficácia do combate das forças armadas da Coroa; v) o bem-estar económico do Reino Unido; vi) as negociações com o titular dos dados; vii) investigação científica ou histórica ou fins estatísticos; viii) arquivo de interesse público. *Explanatory Framework for Adequacy Discussions, section H: National security* (Secção H do quadro explicativo do Reino Unido para debates de adequação: segurança nacional), p. 13, ver a nota de rodapé 31.

proteção de dados seriam suscetíveis de prejudicar o interesse específico em questão. Como tal, a utilização de uma isenção deverá sempre ser justificada e dever-se-á referir o prejuízo relevante que seria suscetível de ocorrer no caso individual. As isenções com base na categoria apenas podem ser invocadas relativamente à categoria de dados específica e definida de modo circunscrito à qual é concedida a isenção. A sua finalidade e efeito são semelhantes a várias das exceções previstas no RGPD do Reino Unido (no *schedule 2* do DPA 2018) que, por sua vez, refletem as limitações previstas no artigo 23.º do RGPD.

(133) No seguimento do disposto anteriormente, estão previstas restrições e condições ao abrigo das disposições legais aplicáveis do Reino Unido, conforme igualmente interpretado pelos tribunais e pelo comissário para a informação, de modo a garantir que essas isenções e restrições permanecem dentro dos limites daquilo que é necessário e proporcionado para proteger a segurança nacional.

3.2 **Acesso e utilização pelas autoridades públicas do Reino Unido para efeitos de aplicação do direito penal**

(134) O direito do Reino Unido impõe uma série de limitações ao acesso e à utilização de dados pessoais para efeitos de aplicação da lei e prevê mecanismos de recurso e supervisão neste domínio, que estão em conformidade com os requisitos referidos nos considerandos 113 a 115 da presente decisão. As secções apresentadas de seguida descrevem as condições nas quais esse acesso pode ser efetuado e as garantias aplicáveis à utilização desses poderes.

3.2.1 *Bases jurídicas e limitações/garantias aplicáveis*

(135) Nos termos do princípio de licitude garantido na *section 35* do DPA 2018, o tratamento de dados pessoais para efeitos de aplicação da lei só é lícito se estiver previsto na lei e se o titular dos dados tiver dado o seu consentimento ao tratamento para essa finalidade ([181]) ou o tratamento for necessário ao exercício de funções de uma autoridade competente para essa finalidade.

3.2.1.1 Mandados de busca e ordens de entrega

(136) O quadro jurídico do Reino Unido autoriza a recolha de dados pessoais dos operadores comerciais, incluindo aqueles que tratariam dados transferidos da UE ao abrigo da presente decisão de adequação, para efeitos de aplicação do direito penal, com base em mandados de busca ([182]) e ordens de entrega ([183]).

(137) Os mandados de busca são emitidos por um tribunal, por norma mediante pedido do responsável de investigação. Estes mandados permitem que um responsável aceda às instalações para procurar materiais ou pessoas importantes para a sua investigação e guarde qualquer coisa que esteja autorizada no âmbito da busca, incluindo documentos ou materiais relevantes que incluam dados pessoais ([184]). Uma ordem de entrega, que também deve ser emitida por um tribunal, exige que a pessoa especificada no mesmo entregue ou dê acesso aos materiais que se encontram na sua posse ou sobre os quais exerce controlo. O requerente deve justificar perante o tribunal por que motivo o mandado ou a ordem é necessário e por que motivo é do interesse público. Existem vários poderes

([181]) A utilização do consentimento não parece relevante num cenário de adequação, uma vez que, numa situação de transferência, os dados não terão sido diretamente recolhidos de um titular de dados da UE sujeito a uma autoridade de aplicação da lei do Reino Unido com base no consentimento.

([182]) Para a base jurídica relevante, consultar as *sections 8* e seguintes do *PACE 1984* (no caso da Inglaterra e do País de Gales), as *sections 10* e seguintes do *Police and Criminal Evidence (Northern Ireland) Order 1989* [Ordem de 1989 sobre as Provas Policiais e Criminais (Irlanda do Norte)] e, no caso da Escócia, é obtida no direito comum (ver a *section 46* do *Criminal Justice (Scotland) Act 2016* [Lei de 2016 relativa à Justiça Criminal (Escócia)] e a *section 23B* do *Criminal Law (Consolidation) (Scotland)* [Direito Penal (Consolidação) (Escócia)]. Para um mandado de busca emitido após a detenção, a base jurídica é a *section 18* do *PACE 1984* (no caso da Inglaterra e do País de Gales), as *sections 20* e seguintes do *Police and Criminal Evidence Order (Northern Ireland) 1989* e, no caso da Escócia, é obtida no direito comum (ver a *section 46* do *Criminal Justice (Scotland) Act 2016*). As autoridades do Reino Unido esclareceram que os mandados de busca são emitidos por um tribunal mediante pedido do responsável de investigação. Permitem que um responsável aceda às instalações para procurar materiais ou pessoas importantes para a sua investigação; frequentemente, para a execução do mandado, é necessária a assistência de um polícia.

([183]) Quando a investigação diz respeito ao branqueamento de capitais (incluindo os processos de perda e de cobrança), a base jurídica relevante para solicitar uma ordem de entrega são as *sections 345* e seguintes para a Inglaterra, o País de Gales e a Irlanda do Norte e as *sections 380* e seguintes do *Proceeds of Crime Act 2002* (Lei de 2002 relativa aos Produtos do Crime) para a Escócia. Quando a investigação diz respeito a outras questões que não o branqueamento de capitais, a *section 9* e o *schedule 1* do *PACE 1984* para a Inglaterra e o País de Gales e a *section 10* e seguintes do *Police and Criminal Evidence Order (Northern Ireland) 1989* para a Irlanda do Norte preveem um pedido de ordem de entrega. No caso da Escócia, é obtido no direito comum (ver a *section 46* do *Criminal Justice (Scotland) Act 2016*) e a *section 23B* do *Criminal Law (Consolidation) (Scotland)*. As autoridades do Reino Unido esclareceram que uma ordem de entrega exige que a pessoa especificada no mesmo entregue ou dê acesso aos materiais que se encontram na sua posse ou sobre os quais exerce controlo (ver o n.º 4 do *schedule 1* do *PACE 1984*).

([184]) Por exemplo, o *PACE 1984* inclui poderes para apreender e guardar qualquer coisa que esteja autorizada no âmbito da busca, em conformidade com o disposto nas secções 8 e 18.

legais que autorizam a emissão de mandados de busca e de ordens de entrega. Cada disposição tem o seu próprio conjunto de condições legais, que devem ser cumpridas no caso de um mandado ([185]) ou de uma ordem de entrega ([186]) que será emitida.

(138) Os mandados de busca e as ordens de entrega podem ser contestados por controlo jurisdicional ([187]).No que diz respeito às garantias, todas as autoridades de aplicação da lei que se enquadram no âmbito da parte 3 do DPA 2018,

([185]) Por exemplo, as *sections 8* e *18* do PACE regulam respetivamente o poder de um julgado de paz para autorizar um mandado e de um agente da polícia para efetuar uma busca numa propriedade. No primeiro caso (*section 8*), antes de emitir um mandado, um julgado de paz deve, em primeiro lugar, certificar-se de que existem motivos razoáveis para acreditar que: i) foi cometido um crime grave; ii) existem materiais nas instalações suscetíveis de terem um valor importante (individualmente ou em conjunto com outros materiais) para a investigação do crime; iii) os materiais são suscetíveis de serem provas importantes; iv) não é composto por ou inclui artigos sujeitos a privilégio legal, materiais excluídos ou materiais de procedimentos especiais; e v) não seria possível conseguir a entrada sem a utilização de um mandado. No segundo caso, a *section 18* permite que um agente policial realize uma busca nas instalações de uma pessoa detida por um crime grave, de modo a procurar materiais que não estejam sujeitos a privilégio legal, caso tenha motivos razoáveis para suspeitar que existem provas nas instalações relacionadas com esse crime ou com outro crime grave semelhante ou associado. Essa busca deve ser limitada a encontrar esses materiais e deve ser autorizada, por escrito, por um agente da polícia com um cargo não inferior a inspetor, a não ser que seja necessária para a investigação do crime. Nesse caso, um agente com um cargo não inferior a inspetor, deve ser informado assim que possível após a realização da busca. Os motivos para a busca e a natureza das provas devem ser registados. Além disso, as *sections 15* e *16* do *PACE 1984* preveem garantias legais que devem ser seguidas ao pedir um mandado de busca. A *section 15* especifica os requisitos aplicáveis à obtenção de um mandado de busca (incluindo os conteúdos do pedido efetuado pelo agente da polícia e o facto de o mandado ser obrigado a especificar, entre outras coisas, a aprovação da sua emissão e identificar, dentro do possível, os artigos e as pessoas em causa e a instalações que serão objeto de uma busca). A *section 16* regula a forma como uma busca autorizada por um mandado deve ser realizada [por exemplo: a *section 16(5)* estabelece que o responsável que executa o mandado deve dar uma cópia do mandado ao ocupante; a *section 16(11)* exige que o mandado, depois de executado, seja conservado durante um período de 12 meses; A *section 16(12)* garante o direito conferido ao ocupante de inspecionar o mandado durante esse período, caso pretenda]. Estas secções ajudam a garantir o cumprimento do artigo 8.º da CEDH (ver, por exemplo, *Kent Pharmaceuticals/Director of the Serious Fraud Office* [2002] EWHC 3023 (QB) a [30] por Lord Woolf CJ). Em resultado do incumprimento destas garantias, a busca pode ser declarada ilícita [os exemplos incluem *R (Brook)/Preston Crown Court* [2018] EWHC 2024 (Admin), [2018] ACD 95; *R (Superior Import/Export Ltd)/Revenue and Customs Commissioners* [2017] EWfHC 3172 (Admin), [2018] Lloyd's Rep FC 115; e *R (F)/Blackfriars Crown Court* [2014] EWHC 1541 (Admin)]. As *sections 15* e *16* do *PACE 1984* são completadas pelo Código B do PACE, um código de boas práticas que regula o exercício dos poderes policiais para realizar buscas nas instalações.

([186]) Por exemplo, ao emitir uma ordem de entrega ao abrigo do *Proceeds of Crime Act 2002*, para além da necessidade de ter motivos razoáveis para cumprir as condições estabelecidas na *section 346(2)* do *Proceeds of Crime Act*, devem existir motivos razoáveis de que a pessoa se encontra na posse dos materiais especificados ou que exerce controlo sobre os mesmos e que os materiais são suscetíveis de terem um valor importante. Além disso, outro requisito para a emissão de uma ordem de entrega é que devem existir motivos razoáveis para acreditar que é do interesse público que os materiais sejam entregues ou que seja concedido o acesso aos mesmos, tendo em conta a) o possível benefício para a investigação em caso de obtenção dos materiais; e b) as circunstâncias em que a pessoa especificada no pedido como estando aparentemente na posse dos materiais ou a exercer controlo sobre os mesmos detém as suas informações. De igual forma, um tribunal que esteja a apreciar um pedido de uma ordem de entrega ao abrigo do *schedule 1* do *PACE 1984* deve certificar-se de que são cumpridas condições específicas. Em particular, o *schedule 1* do PACE estabelece dois conjuntos de condições alternativos e separados, um dos quais deve ser cumprido antes que um juiz possa emitir uma ordem de entrega. O primeiro conjunto exige que o juiz tenha motivos razoáveis para acreditar i) que foi cometido um crime grave; ii) os materiais procurados nas instalações são compostos por ou incluem procedimentos especiais, mas não materiais excluídos; iii) são suscetíveis de ter um valor importante para a investigação, quer individualmente, quer em conjunto com outros materiais; iv) e são suscetíveis de ser provas importantes; v) tentou utilizar-se outros métodos para a obtenção dos materiais ou não houve essa tentativa porque o seu fracasso era seguro; e vi) depois de considerado o benefício para a investigação e as circunstâncias nas quais a pessoa singular possui esses materiais, é do interesse público que os materiais sejam entregues ou que seja concedido o acesso aos mesmos. O segundo conjunto de condições exige: i) existem materiais nas instalações compostos por materiais de procedimentos especiais ou excluídos; ii) se não fosse pela proibição das buscas realizadas com base na legislação aprovada antes do PACE em questão de materiais de procedimentos especiais, excluídos ou de privilégio legal, era possível emitir um mandado de busca para os materiais; e iii) teria sido adequado fazê-lo.

([187]) O controlo jurisdicional é o procedimento jurídico que permite que as decisões de um organismo público possam ser contestadas no *High Court*. Os tribunais «analisam» a decisão que está a ser contestada e decidem se é possível determinar que a decisão tem falhas do ponto de vista legal, tendo em conta os conceitos/princípios do direito público. As razões principais para o controlo jurisdicional são, nomeadamente, a ilegalidade, a irracionalidade, a desadequação processual, as expetativas legítimas e os direitos humanos. Na sequência de um controlo jurisdicional correto, um tribunal pode ordenar várias vias de recurso diferentes; a via mais comum é uma ordem de anulação (que adiaria ou cancelaria a decisão original, ou seja, a decisão de emitir um mandado de busca). Em determinadas circunstâncias, isto pode ainda incluir a atribuição de uma indemnização. Para mais informações sobre o controlo jurisdicional no Reino Unido, consultar a publicação *Judge Over Your Shoulder – a guide to good decision-making* (Um juiz por cima do seu ombro — um guia para tomar boas decisões) do *Government Legal Department*, disponível na seguinte ligação: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/746170/JOYS-OCT-2018.pdf

apenas podem aceder aos dados pessoais – que são uma forma de tratamento – em conformidade com os princípios e os requisitos estabelecidos no DPA 2018 (ver os considerandos (122) e (124) above). Como tal, um pedido efetuado por uma autoridade de aplicação da lei deve cumprir o princípio segundo o qual as finalidades do tratamento devem ser específicas, explícitas e legítimas ([188]) e os dados pessoais tratados por uma autoridade competente devem ser relevantes para essa finalidade e não excessivos ([189]).

3.2.1.2 Poderes de investigação para efeitos da aplicação da lei

(139) Para efeitos de prevenção ou de deteção unicamente de criminalidade grave ([190]), determinadas autoridades de aplicação da lei, por exemplo a *National Crime Agency* ou o chefe da autoridade policial ([191]), podem utilizar poderes de investigação específicos ao abrigo do IPA 2016. Neste caso, as garantias previstas no IPA 2016 serão aplicáveis para além das previstas na parte 3 do DPA 2018. Os poderes de investigação específicos a que essas autoridades de aplicação da lei podem recorrer são os seguintes: interceções direcionadas (parte 2 do IPA 2016), aquisição de dados de comunicações (parte 3 do IPA 2016), conservação de dados de comunicações (parte 4 do IPA 2016) e interferência direcionada em equipamentos (parte 5 do IPA 2016). A interceção abrange a aquisição dos conteúdos de uma comunicação ([192]), ao passo que a aquisição e a conservação de dados de comunicações não tem como objetivo obter os conteúdos da comunicação, mas sim obter o «quem», o «quando», o «onde» e o «como» da comunicação. Isto abrange, por exemplo, a hora e a duração de uma comunicação, o número de telefone ou endereço eletrónico do autor e do destinatário da comunicação e, por vezes, a localização dos dispositivos a partir dos quais foi efetuada a comunicação, o assinante de um serviço telefónico ou uma fatura discriminada ([193]). A interferência com os equipamentos constitui um conjunto de técnicas utilizadas para obter uma série de dados de equipamentos, incluindo computadores, tablets e telemóveis inteligentes, bem como cabos, fios e dispositivos de armazenamento ([194]).

(140) Os poderes de interceção direcionada também podem ser utilizados quando forem «necessários para a aplicação das disposições de um instrumento de assistência mútua da UE ou um acordo de assistência mútua internacional» (o chamado «mandado de assistência mútua» ([195])). Os mandados de assistência mútua apenas são emitidos em relação à interceção e não à aquisição de dados de comunicações ou à interferência com os equipamentos. Estes poderes direcionados são regulados no *Investigatory Powers Act 2016* (Lei de 2016 relativa aos Poderes de Investigação) (IPA 2016) ([196]), que, 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, apresentam a base jurídica e estabelecem as limitações e as garantias aplicáveis para a utilização desses poderes. O IPA 2016 estabelece ainda o regime de utilização dos poderes de investigação em larga escala, embora as autoridades de aplicação da lei não disponham destes poderes (apenas podem ser utilizados pelas agências de informações) ([197]).

([188]) *Section 36(1)* do DPA 2018 do Reino Unido.
([189]) *Section 37* do DPA 2018 do Reino Unido.
([190]) A *section 263(1)* do IPA 2016 descreve «crimes graves» como infrações que, quando cometidas por um adulto sem condenações anteriores, podem levar a uma pena de prisão de três anos ou mais ou quando a conduta envolve o recurso à violência, resulta em benefícios económicos avultados ou é realizada por um grande número de pessoas. Além disso, para efeitos da aquisição de dados de comunicações prevista na parte 4 do IPA 2016, a *section 87(10B)* descreve um «crime grave» como um crime que pode conduzir a uma pena de prisão de 12 meses ou mais ou uma infração cometida por alguém que não seja uma pessoa singular ou que envolve, como parte integrante da mesma, o envio de uma comunicação ou uma violação da privacidade de um indivíduo.
([191]) As autoridades de aplicação da lei apresentadas de seguida podem solicitar um mandado de interceção direcionada: o diretor-geral da *National Crime Agency*, o comissário da polícia de Metropolis, o *Chief Constable* da polícia da Irlanda do Norte, o *Chief Constable* da polícia da Escócia, o comissário do departamento *Her Majesty's Revenue and Customs*, o chefe do *Defence Intelligence* e uma pessoa que seja uma autoridade competente de um país ou território fora do Reino Unido para efeitos de um instrumento de assistência mútua da UE ou um acordo de assistência mútua internacional [*section 18(1)* do IPA 2016].
([192]) Ver a *section 4* do IPA 2016.
([193]) Ver a *section 261(5)* do IPA 2016 e o *Code of Practice on Bulk Acquisition of Communications Data* (código de prática sobre a aquisição em larga escala de dados de comunicações), disponível na seguinte ligação: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715477/Bulk_Communications_Data_Code_of_Practice.pdf, secção 2.9.
([194]) *Code of Practice on Equipment Interference*, disponível na seguinte ligação: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715479/Equipment_Interference_Code_of_Practice.pdf, ponto 2.2.
([195]) Um mandado de assistência mútua autoriza as autoridades do Reino Unido a prestar assistência a uma autoridade fora do território do Reino Unido para efeitos de interceção e divulgação do material intercetado a essa autoridade, de acordo com um instrumento de assistência mútua internacional [*section 15(4)* do IPA 2016].
([196]) O *Investigatory Powers Act 2016* (consultar: 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.
([197]) *Sections 138(1), 158(1), 178(1), 199(1)* do IPA 2016.

(141) De modo a exercer estes poderes, as autoridades precisam de obter um mandado ([198]) emitido por uma autoridade competente ([199]) e aprovado por um comissário judicial independente ([200]) [o chamado procedimento «*double-lock*» (dupla segurança)]. A obtenção desse mandado está sujeita a um teste de necessidade e proporcionalidade ([201]). Uma vez que estes poderes de investigação específicos previstos no IPA 2016 são os mesmos que os que estão disponíveis para as agências de segurança nacionais, as condições, as limitações e as garantias aplicáveis a esses poderes são descritas na secção referente ao acesso e à utilização de dados pessoais pelas autoridades públicas do Reino Unido para efeitos de segurança nacional (ver os considerandos 177 e seguintes).

3.2.2 *Utilização adicional das informações recolhidas*

(142) A partilha de dados por uma autoridade de aplicação da lei com outra autoridade para outros fins que não aqueles para os quais foram originalmente recolhidos (a chamada «transferência subsequente») está sujeita a determinadas condições.

(143) À semelhança do disposto no artigo 4.º, n.º 2, da Diretiva (UE) 2016/680, a *section 36(3)* do DPA 2018 permite que os dados pessoais recolhidos por uma autoridade competente para efeitos de aplicação da lei sejam tratados posteriormente (pelo responsável pelo tratamento original ou por outro responsável pelo tratamento) para qualquer outra finalidade de aplicação da lei, desde que o responsável pelo tratamento esteja autorizado por lei a efetuar o tratamento dos dados com outra finalidade e o tratamento seja necessário e proporcional a essa finalidade ([202]). Neste caso, todas as garantias previstas na parte 3 do DPA 2018, a que se referem os considerandos 122 e 124, são aplicáveis ao tratamento efetuado pela autoridade que os recebe.

(144) Na ordem jurídica do Reino Unido, diferentes leis permitem explicitamente a transferência subsequente. Em particular, i) o *Digital Economy Act 2017* (Lei de 2017 relativa à Economia Digital) permite a partilha entre as autoridades públicas para várias finalidades, por exemplo, em caso de fraude contra o setor público que implicasse uma perda ou risco de perda para as autoridades públicas ([203]) ou em caso de dívida com uma autoridade pública ou a Coroa ([204]); ii) o *Crime and Courts Act 2013* (Lei de 2013 relativa ao Crime e aos Tribunais) que permite a partilha de informações com a *National Crime Agency* (NCA) ([205]) para o combate, a investigação e a repressão da criminalidade grave e organizada; iii) o *Serious Crime Act 2007* (Lei de 2007 relativa à Criminalidade Grave) que permite que as autoridades públicas divulguem informações às organizações antifraude para efeitos de prevenção da fraude ([206]).

(145) Estas leis prescrevem explicitamente que a partilha de informações deve cumprir os princípios estabelecidos no DPA 2018. Além disso, o *College of Policing* emitiu uma Prática Profissional Autorizada para a partilha de informações ([207]), de modo a auxiliar a polícia no cumprimento das suas obrigações de proteção dos dados previstas no RGPD do Reino Unido, no DPA e no *Human*

([198]) 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.

([199]) 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* do 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* do IPA 2016) pode emitir um mandado de acordo com as condições estabelecidas na *section 106* do IPA 2016.

([200]) Os comissários judiciais auxiliam o comissário para os poderes de investigação, um organismo independente que exerce funções de supervisão, na utilização dos poderes de investigação pelas agências de informações (para mais informações, ver o considerando 162 e seguintes).

([201]) Ver, em particular, as *sections 19* e *23* do IPA 2016.

([202]) *Section 36(3)* do DPA 2018.

([203]) *Section 56* do *Digital Economy Act 2017*, disponível na seguinte ligação: https://www.legislation.gov.uk/ukpga/2017/30/section/56

([204]) *Section 48* do *Digital Economy Act 2017*.

([205]) *Section 7* do *Crime and Courts Act 2013*, disponível na seguinte ligação: https://www.legislation.gov.uk/ukpga/2013/22/section/7

([206]) *Section 68* do *Serious Crime Act 2007*, disponível na seguinte ligação: https://www.legislation.gov.uk/ukpga/2007/27/contents

([207]) Prática Profissional Autorizada para a partilha de informações, disponível na seguinte ligação: https://www.app.college.police.uk/app-content/information-management/sharing-police-information

Rights Act 1998. O cumprimento da partilha do quadro jurídico aplicável para a proteção de dados está, obviamente, sujeito a controlo jurisdicional ([208]).

(146) Além disso, à semelhança do disposto no artigo 9.º da Diretiva (UE) 2016/680, o DPA 2018 prevê que os dados pessoais recolhidos para efeitos de aplicação da lei podem ser objeto de tratamento para outro fim que não a aplicação da lei quando o tratamento é autorizado por lei ([209]).

(147) Este tipo de partilha abrange dois cenários: 1) quando a autoridade de aplicação do direito penal partilha dados com uma autoridade que não uma de aplicação do direito penal, mas que não é uma agência de informações (como, por exemplo, uma autoridade fiscal ou financeira, uma autoridade da concorrência, uma organização de subsídios para jovens, etc.); e 2) quando uma autoridade de aplicação do direito penal partilha dados com uma agência de informações. No primeiro cenário, o tratamento de dados pessoais encontra-se abrangido pelo âmbito de aplicação do RGPD do Reino Unido, bem como na parte 2 do DPA 2018. A Comissão avaliou as garantias previstas no RGPD do Reino Unido e na parte 2 do DPA 2018 nos considerandos 12 a 111 e chegou à conclusão de que o Reino Unido assegura um nível adequado de proteção dos dados pessoais transferidos da União Europeia para o Reino Unido, no âmbito do Regulamento (UE) 2016/679.

(148) No segundo cenário, no que diz respeito à partilha de dados recolhidos de uma agência de informações por uma autoridade de aplicação do direito penal para efeitos de segurança nacional, a base jurídica que autoriza essa partilha é a *section 19* do *Counter Terrorism Act 2008* (Lei de 2008 relativa ao Combate ao Terrorismo) (CTA 2008) ([210]). Ao abrigo desta lei, qualquer pessoa pode facultar informações a quaisquer serviços de informações para efeitos de cumprimento das funções desse serviço, incluindo as funções de «segurança nacional».

(149) No que diz respeito às condições em que os dados podem ser partilhados para efeitos de segurança nacional, o *Intelligence Services Act* (Lei relativa ao Serviço de Informações) ([211]) e o *Security Service Act* (Lei relativa ao Serviço de Segurança) ([212]) limitam a capacidade dos serviços de informações de obterem dados estritamente necessários para cumprirem as suas obrigações legais. As agências de aplicação da lei que procuram partilhar dados com os serviços de informações deverão ter em consideração uma série de fatores/limitações, para além das funções legais das agências que são estabelecidas no *Intelligence Services Act* e no *Security Service Act* ([213]). A *section 20* do CTA 2008 clarifica que qualquer partilha de dados efetuada nos termos da *section 19* deve cumprir a legislação em matéria de proteção de dados; o que significa que todas as limitações e requisitos estabelecidos na parte 3 do DPA 2018 são aplicáveis. Além disso, uma vez que, para efeitos do *Human Rights Act 1998*, as autoridades competentes são autoridades públicas, estas devem assegurar o cumprimento dos direitos da Convenção, incluindo o artigo 8.º da CEDH. Estes limites asseguram que qualquer partilha de dados entre as agências de aplicação da lei e os serviços de informações cumprem a legislação em matéria de proteção de dados e a CEDH.

([208]) Ver, por exemplo, o processo *M, R/Chief Constable of Sussex Police* [2019] EWHC 975 (Admin), no qual foi pedido ao *High Court* que tivesse em consideração a partilha de dados entre a polícia e uma parceria para o combate à criminalidade empresarial [*Business Crime Reduction Partnership*, BCRP], uma organização habilitada para gerir regimes de notificações de exclusão, que proíbe as pessoas de entrar nas instalações comerciais dos seus membros. O tribunal analisou a partilha de dados, que estava a decorrer com base num acordo que tinha como finalidade proteger o público e prevenir a criminalidade e, em última instância, concluiu que a maioria dos aspetos da partilha de dados era lícita, à exceção de algumas informações sensíveis partilhadas entre a polícia e o BCRP. Outro exemplo é o processo *Cooper/NCA* [2019] EWCA Civ 16 no qual o Court of Appeal (Tribunal de Recurso) analisou a partilha de dados entre a polícia e a Serious Organised Crime Agency (SOCA), uma agência de aplicação da lei que atualmente faz parte da NCA.

([209]) *Section 36(4)* do DPA 2018.

([210]) *Counter Terrorism Act 2008*, disponível na seguinte ligação: https://www.legislation.gov.uk/ukpga/2008/28/section/19

([211]) *Intelligence Services Act 1994*, disponível na seguinte ligação: https://www.legislation.gov.uk/ukpga/1994/13/contents

([212]) *Security Service Act 1989*, disponível na seguinte ligação: https://www.legislation.gov.uk/ukpga/1989/5/contents

([213]) A *section 2(2)* do *Intelligence Services Act 1994* (Lei de 1994 relativa aos Serviços de Informações) estabelece que «[o] diretor do serviço de informações é responsável pela eficácia desse serviço e cabe-lhe garantir — a) que existem mecanismos que garantem que o serviço de informações apenas obtém as informações estritamente necessárias ao exercício adequado das suas funções e que o serviço de informações apenas divulga as informações estritamente necessárias — i) para esse efeito; ii) no interesse da segurança nacional; iii) para efeitos de prevenção ou deteção da criminalidade grave; ou iv) para efeitos de processos penais; e b) que o serviço de informações não toma nenhuma medida para concretizar os interesses de algum partido político do Reino Unido», ao passo que a *section 2(2)* do *Security Service Act 1989* prevê que «[o] diretor-geral é responsável pela eficácia do serviço e cabe-lhe a ele garantir — a) que existem mecanismos que garantem que o serviço de informações apenas obtém as informações estritamente necessárias ao exercício adequado das suas funções e que o serviço de informações apenas divulga as informações estritamente necessárias para esse efeito ou para efeitos de prevenção ou deteção da [criminalidade grave ou para efeitos de processos penais]; e b) que o serviço não toma nenhuma medida para concretizar os interesses de algum partido político; e c) que existem mecanismos acordados com o diretor-geral da *National Crime Agency* para a coordenação das atividades do serviço, nos termos da *section 1(4)* da presente lei, com as atividades das forças policiais, a National Crime Agency e outras agências de aplicação da lei».

(150) São aplicáveis requisitos específicos quando uma autoridade competente pretende partilhar com as autoridades de aplicação da lei de um país terceiro os dados pessoais objeto de tratamento ao abrigo da parte 3 do DPA 2018 ([214]). Em particular, essas transferências podem ocorrer quando têm por base regulamentos de adequação efetuados pelo ministro da tutela ou, à falta desses regulamentos, devem ser asseguradas garantias adequadas. A section 75 do DPA 2018 determina a existência de garantias adequadas quando estas se encontram estabelecidas por um instrumento jurídico que vincula o destinatário pretendido ou caso o responsável pelo tratamento, depois de ter avaliado todas as circunstâncias das transferências desse tipo de dados pessoais para o país terceiro ou organização internacional, conclua que existem garantias adequadas para proteger os dados.

(151) Caso uma transferência não tenha por base um regulamento de adequação ou garantias adequadas, só poderá ser efetuada em circunstâncias determinadas e específicas, denominadas «circunstâncias especiais» ([215]). Esse é o caso quando a transferência é necessária: a) para defender os interesses vitais do titular dos dados ou de outra pessoa; b) para proteger os interesses legítimos do titular dos dados; c) para a prevenção de uma ameaça imediata e grave contra a segurança pública de um Estado-Membro ou de um país terceiro; d) em casos individuais para efeitos de aplicação da lei; ou e) em casos individuais para efeitos legais (como processos penais ou para obter aconselhamento jurídico). Importa salientar que as alíneas d) e e) não são aplicáveis caso os direitos e liberdades do titular dos dados se sobreponham ao interesse público da transferência. Este conjunto de circunstâncias corresponde a situações e condições específicas que se qualificam como «derrogações», nos termos do artigo 38.º da Diretiva (UE) 2016/680.

(152) Além disso, quando os materiais adquiridos pelas autoridades de aplicação da lei ao abrigo de um mandado que autoriza a utilização da interceção ou da interferência com os equipamentos são entregues a um país terceiro, o IPA 2016 impõe garantias adicionais. Em particular, essa divulgação, definida como «divulgação no estrangeiro», apenas é permitida se a autoridade emissora considerar que existem mecanismos adequados e específicos que limitam o número de pessoas a quem os dados são divulgados, a medida em que os materiais são divulgados ou disponibilizados, bem como a medida em que qualquer um dos materiais é copiado e o número de cópias efetuadas. Além disso, a autoridade emissora pode considerar que são necessários mecanismos adequados para garantir que todas as cópias efetuadas de qualquer uma das partes desses materiais são destruídas assim que deixar de haver motivos válidos para a respetiva conservação (se não forem destruídas antes) ([216]).

(153) Por último, no futuro podem ocorrer formas específicas de transferências ulteriores do Reino Unido para os Estados Unidos, com base no «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» ou «Acordo») ([217]), celebrado em outubro de 2019 ([218]). Apesar de o Acordo RU-EUA ainda não ter entrado em vigor [aquando da adoção da presente decisão], a sua previsível entrada em vigor pode afetar as transferências ulteriores para os EUA de dados transferidos primeiro para o Reino Unido com base na decisão. Mais especificamente, 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 eletrónicos emitidos pelas autoridades de aplicação da lei competentes dos EUA e aplicáveis no Reino Unido ao abrigo do presente acordo depois de o mesmo entrar em vigor. Por estes motivos, a avaliação das condições e das garantias ao abrigo das quais essas ordens podem ser emitidas e executadas é relevante para a presente decisão.

([214]) Ver parte 3, capítulo 5, do DPA 2018.

([215]) *Section 76* do DPA 2018.

([216]) *Section 54* e *section 130* do IPA 2016. As autoridades emissoras devem ter em conta a necessidade de impor garantias específicas aos materiais entregues a autoridades estrangeiras, de forma a certificarem-se de que os dados estão sujeitos a garantias no que diz respeito à conservação, destruição e divulgação de dados semelhantes às impostas nas *sections 53* e *129* do IPA 2016.

([217]) *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), 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

([218]) Este é o primeiro acordo celebrado ao abrigo do *Clarifying Lawful Overseas Use of Data (CLOUD) Act* (Lei relativa à Clarificação da Utilização Legítima de Dados no Estrangeiro) dos EUA. O *CLOUD Act* dos Estados Unidos é uma lei federal norte-americana adotada em 23 de março de 2018 que clarifica, através de uma alteração do *Stored Communications Act* (Lei relativa às Comunicações Armazenadas) de 1986, que os prestadores de serviços dos EUA são obrigados a cumprir as ordens dos EUA de divulgação de dados com ou sem conteúdos, independentemente do local onde esses dados estão armazenados. O *CLOUD Act* permite igualmente a celebração de acordos executivos com governos estrangeiros, segundo os quais os prestadores de serviços dos EUA poderiam entregar dados com conteúdos diretamente a esses governos estrangeiros (poderá consultar o texto do *CLOUD Act* na seguinte ligação: https://www.congress.gov/115/bills/s2383/BILLS-115s2383is.pdf).

(154) A este respeito, importa salientar que, em primeiro lugar, no que se refere ao respetivo âmbito de aplicação material, o acordo só é aplicável a crimes que são puníveis com uma pena máxima de pelo menos três anos (definidos como «crimes graves») ([219]), incluindo a «atividade terrorista». Em segundo lugar, ao abrigo do presente acordo, os dados objeto de tratamento na outra jurisdição apenas podem ser obtidos após uma «[o]rdem […] sujeita a apreciação ou supervisão ao abrigo do direito nacional da parte emissora por um tribunal, juiz, magistrado ou outra autoridade independente antes ou durante os processos relativos à execução da Ordem» ([220]). Em terceiro lugar, qualquer ordem deve «ter como base os requisitos de uma justificação razoável que tenha como base factos articuláveis e credíveis, a particularidade, a legalidade e a gravidade relativas à conduta sob investigação» ([221]) e «ser direcionada a contas específicas, bem como identificar uma pessoa específica, conta, endereço ou dispositivo pessoal ou qualquer outro identificador específico» ([222]). Em quarto lugar, os dados obtidos ao abrigo do presente Acordo beneficiam de proteções equivalentes às garantias específicas previstas no chamado «Acordo-Quadro UE-EUA» ([223]) — um acordo global de proteção de dados celebrado em dezembro de 2016 pela UE e os EUA e que estabelece as garantias e os direitos aplicáveis às transferências de dados no domínio da cooperação para a aplicação da lei — que estão todos incluídos no presente acordo numa base *mutatis mutandis*, para ter em conta a natureza específica das transferências (ou seja, transferências de operadores particulares para uma autoridade de aplicação da lei, em vez de transferências entre autoridades de aplicação da lei) ([224]). O Acordo RU-EUA prevê especificamente a aplicação de proteções equivalentes às oferecidas pelo Acordo-Quadro UE-EUA «a todos os dados pessoais elaborados na execução das ordens sujeitas ao acordo, a fim de produzir proteções equivalentes» ([225]).

(155) Como tal, os dados transferidos para as autoridades dos EUA ao abrigo do Acordo RU-EUA devem beneficiar das proteções criadas por um instrumento jurídico da UE, com as adaptações necessárias para refletir a natureza das transferências em questão. As autoridades do Reino Unido confirmaram que as proteções do Acordo-Quadro aplicar-se-ão a todos os dados pessoais elaborados ou conservados ao abrigo do acordo, independentemente da natureza ou do tipo de organismo que realiza o pedido (por exemplo, as autoridades de aplicação da lei federais e estatais nos EUA), para que possam ser oferecidas proteções equivalentes em todos os casos. Contudo, as autoridades do Reino Unido também explicaram que os pormenores sobre a aplicação concreta das garantias em matéria de proteção de dados continuam a ser objeto de discussões entre o Reino Unido e os EUA. No contexto das discussões sobre esta decisão com os serviços da Comissão Europeia, as autoridades do Reino Unido confirmaram que apenas permitirão a entrada em vigor do acordo depois de terem a certeza de que a sua aplicação cumpre as obrigações legais estabelecidas no mesmo, incluindo a clareza no que diz respeito ao cumprimento das normas de proteção de dados aplicáveis aos dados solicitados ao abrigo do presente acordo. Uma vez que a possível entrada em vigor do acordo poderá ter um impacto no nível de proteção avaliado na presente decisão, qualquer informação e futuro esclarecimento relativo à forma como os EUA cumprirão as suas obrigações ao abrigo do acordo deve ser comunicado pelo Reino Unido à Comissão Europeia, assim que estiver disponível e, em qualquer caso, antes da entrada em vigor do acordo, de modo a garantir um controlo adequado da presente decisão, em conformidade com o artigo 45.º, n.º 4, do Regulamento (UE) 2016/679. Será dada especial atenção à aplicação e à adaptação das proteções estabelecidas no Acordo-Quadro para os tipos específicos de transferências abrangidos pelo Acordo RU-EUA.

(156) De um modo mais geral, qualquer desenvolvimento importante no que se refere à entrada em vigor e à aplicação do acordo será devidamente tido em conta no contexto do controlo contínuo da presente decisão, incluindo no que diz respeito às consequências necessárias caso exista alguma indicação de que um nível de proteção essencialmente equivalente deixou de ser assegurado.

3.2.3 *Supervisão*

(157) Dependendo dos poderes utilizados pelas autoridades competentes aquando do tratamento de dados pessoais para efeitos de aplicação da lei (ao abrigo do DPA 2018 ou do IPA 2016), existem diferentes organismos que asseguram a supervisão da utilização destes poderes. Em particular, o comissário para a informação supervisiona o tratamento de

([219]) Artigo 1.º, n.º 14, do acordo.
([220]) Artigo 5.º, n.º 2, do acordo.
([221]) Artigo 5.º, n.º 1, do acordo.
([222]) Artigo 4.º, n.º 5, do acordo. É aplicável uma norma adicional e mais rigorosa no que diz respeito à interceção em tempo real: as ordens devem ter uma duração limitada, que não pode ser superior ao razoavelmente necessário para alcançar as finalidades da ordem, e apenas devem ser emitidas se não for possível obter a mesma informação através de um método menos intrusivo (artigo 5.º, n.º 3, do acordo).
([223]) 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), disponível na seguinte ligação: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:22016A1210(01)&from=PT
([224]) Artigo 9.º, n.º 1, do acordo.
([225]) Artigo 9.º, n.º 1, do acordo.

dados pessoais quando se encontra abrangido pelo âmbito de aplicação da parte 3 do DPA 2018 ([226]). A supervisão independente e judicial da utilização dos poderes de investigação ao abrigo do IPA 2016 é assegurada pelo Gabinete do Comissário para os Poderes de Investigação (IPCO) ([227]) (esta parte é abordada nos considerandos 250 a 255). Além disso, o parlamento e outros organismos garantem uma supervisão adicional.

3.2.3.1 Supervisão da parte 3 do DPA 2018

(158) As funções gerais do comissário para a informação — cuja independência e organização são explicadas no considerando 87 — relativas ao tratamento de dados pessoais que se encontra abrangido pelo âmbito de aplicação da parte 3 do DPA 2018 são estabelecidas no *schedule 13* do DPA 2018. A principal tarefa do ICO é controlar e executar a parte 3 do DPA 2018, bem como promover a sensibilização do público, aconselhar o parlamento, o governo e outras instituições e organismos. A fim de assegurar a independência do poder judicial, o comissário para a informação não está autorizado a exercer as suas funções relativas ao tratamento de dados pessoais efetuado pelos tribunais ou por pessoas singulares no exercício da sua função jurisdicional. Nestas circunstâncias, outros organismos exerceriam as funções de supervisão, conforme explicado nos considerandos 99 a 103.

(159) O comissário possui poderes gerais de investigação, de correção, de autorização e de aconselhamento relativos ao tratamento de dados pessoais aos quais se aplica a parte 3. Em particular, o comissário tem poderes para notificar o responsável pelo tratamento ou o subcontratante de uma alegada violação da parte 3 do DPA 2018, para emitir advertências ou repreensões destinadas a um responsável pelo tratamento ou um subcontratante que tenha violado as disposições da parte 3 da lei, bem como para emitir, por iniciativa própria ou se lhe for solicitado, pareceres dirigidos ao parlamento, ao governo ou a outras instituições e organismos, bem como ao público, sobre qualquer assunto relacionado com a proteção de dados pessoais ([228]).

(160) Além disso, o comissário tem poderes para emitir notificações informativas ([229]), notificações de avaliação ([230]) e notificações de execução ([231]), bem como o poder de aceder aos documentos dos responsáveis pelo tratamento e dos subcontratantes, de aceder às suas instalações ([232]) e de emitir coimas sob a forma de notificações de sanção ([233]). A política de intervenção regulamentar do ICO descreve as circunstâncias em que emite notificações informativas, de avaliação, de execução e de sanção ([234]) [ver ainda o considerando 93 e os considerandos 101 e 102 relativos à decisão de adequação da Diretiva (UE) 2016/680].

(161) De acordo com os seus relatórios anuais mais recentes (2018-2019 ([235]), 2019-2020 ([236])), o comissário para a informação realizou uma série de investigações e tomou medidas de execução relativas ao tratamento de dados pelas autoridades de aplicação da lei. Por exemplo, em outubro de 2019, o comissário realizou uma investigação e publicou um parecer relativo à utilização da tecnologia de reconhecimento facial em locais públicos pelas autoridades de aplicação da lei. A investigação centrou-se, em particular, na utilização das capacidades de reconhecimento facial em tempo real pela polícia da Gales do Sul e pelo *Metropolitan Police Service* (MPS). O comissário para a informação investigou a «matriz dos gangues» do MPS ([237]) e descobriu um conjunto de violações graves da legislação de proteção de dados que poderiam reduzir a confiança do público na matriz e na forma como os dados estavam a ser utilizados. Em novembro de 2018, o comissário para a informação emitiu uma notificação de execução e, subsequentemente, o MPS tomou as medidas necessárias para aumentar a segurança e a responsabilidade e para assegurar que os dados eram utilizados de forma proporcionada. Outro exemplo de uma ação de execução neste domínio é a coima de 325 000 GBP emitida pelo

([226]) *Section 116* do DPA 2018.
([227]) Ver o IPA 2016 e, em particular, a parte 8, capítulo 1.
([228]) *Schedule 13*, n.º 2, do DPA 2018.
([229]) Ordenar que o responsável pelo tratamento e o subcontratante (e, em determinadas circunstâncias, qualquer outra pessoa) prestem as informações necessárias (*section 142* do DPA 2018).
([230]) Permitir a realização de investigações e auditorias, o que poderá exigir que o responsável pelo tratamento ou o subcontratante autorize que o comissário entre nas instalações específicas, inspecione ou analise os documentos ou os equipamentos e entreviste as pessoas responsáveis pelo tratamento dos dados pessoais em nome do responsável pelo tratamento (*section 146* do DPA 2018).
([231]) Permitir o exercício dos poderes de correção, o que exige que os responsáveis pelo tratamento/subcontratantes tomem ou se abstenham de tomar medidas específicas (*section 149* do DPA 2018).
([232]) *Section 154* do DPA 2018.
([233]) *Section 155* do DPA 2018.
([234]) *Regulatory Action Policy*, ver a nota de rodapé 96.
([235]) *Information Commissioner's Annual Report and Financial Statements 2018-19*, ver a nota de rodapé 101.
([236]) *Information Commissioner's Annual Report and Financial Statements 2019-20*, ver a nota de rodapé 82.
([237]) Uma base de dados que registava informações relacionadas com alegados membros de gangues e vítimas de crimes de gangues.

comissário em maio de 2018 contra o Crown Prosecution Service, por ter perdido DVD não encriptados que continham gravações de inquéritos policiais. O comissário para a informação realizou igualmente investigações a temas mais abrangentes, por exemplo, no primeiro semestre de 2020, relativas à utilização da extração de números de telefone para efeitos policiais e ao tratamento dos dados das vítimas pela polícia. Além disso, o comissário está agora a investigar um caso que envolve o acesso das autoridades de aplicação da lei a dados que se encontravam na posse de uma entidade do setor privado, a Clearview AI Inc ([238]).

(162) Para além dos poderes de execução do comissário para a informação descritos nos considerandos 160 e 161, determinadas violações da legislação em matéria de proteção de dados constituem infrações e, como tal, podem ser sujeitas a sanções penais (*section 196* do DPA 2018). Isto aplica-se, por exemplo, à obtenção, divulgação ou conservação de dados pessoais sem o consentimento do responsável pelo tratamento e a divulgação de dados pessoais a outra pessoa sem o consentimento do responsável pelo tratamento ([239]); à reidentificação de informações que são dados pessoais anonimizados sem o consentimento do responsável pelo tratamento que ficou incumbido da anonimização dos dados pessoais ([240]); à obstrução intencional do comissário para impedi-lo de exercer os seus poderes relativamente à inspeção dos dados pessoais, de acordo com as obrigações internacionais ([241]), às declarações falsas em resposta a uma notificação informativa ou à destruição de informações relacionadas com notificações informativas e de avaliação ([242]).

3.2.3.2 Outros organismos de supervisão no domínio da aplicação do direito penal

(163) Além do comissário para a informação, existem vários organismos de supervisão no domínio da aplicação do direito penal com competências específicas pertinentes em matéria de proteção de dados, nomeadamente, por exemplo, o comissário para a conservação e a utilização de materiais biométricos (o «comissário biométrico») ([243]) e o comissário para as câmaras de videovigilância ([244]).

3.2.3.3 Supervisão parlamentar no domínio da aplicação do direito penal

(164) A *Home Affairs Select Committee* (HASC) (comissão especial para os assuntos internos) assegura a supervisão parlamentar no domínio da aplicação da lei. É composta por 11 membros do parlamento, provenientes dos três principais partidos políticos e está incumbida de examinar as despesas, a administração e a política do Ministério da Administração Interna e dos organismos públicos associados, isto é, incluindo a polícia e a NCA, cujo trabalho pode ser analisado minuciosamente pela comissão ([245]).

([238]) Ver a demonstração do ICO, disponível na seguinte ligação: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/07/oaic-and-ico-open-joint-investigation-into-clearview-ai-inc/

([239]) *Section 170* do DPA 2018.

([240]) *Section 171* do DPA 2018.

([241]) *Section 119(6)* do DPA 2018.

([242]) Durante o exercício financeiro que abrange o período de 1 de abril de 2019 a 31 de março de 2020, as investigações do ICO resultaram em quatro advertências e oito ações penais. Estes casos foram julgados ao abrigo da *section 55* do *Data Protection Act 1998*, da *section 77* do *Freedom of Information Act 2000* e da *section 170* do *Data Protection Act 2018*. Em 75% dos casos, os arguidos declararam-se culpados e não houve necessidade de julgamentos morosos e de incorrer em custos associados. *Information Commissioner's Annual Report and Financial Statements 2019-2020* (Relatório anual e demonstrações financeiras do comissário para a informação), ver a nota de rodapé 87, p. 40.

([243]) O comissário biométrico foi criado pelo *Protection of Freedoms Act 2012* (Lei de 2012 relativa à Proteção das Liberdades) (PoFA) (ver: https://www.legislation.gov.uk/ukpga/2012/9/contents). que, designadamente, decide se a polícia pode ou não conservar os registos dos perfis de ADN e impressões digitais de pessoas detidas, mas não acusadas, por infrações graves (*section 63G* do PACE 1984). Além disso, o comissário biométrico tem a responsabilidade geral de reavaliar a conservação e utilização de ADN e impressões digitais e a conservação por motivos de segurança nacional [*section 20(2)*, do PoFA 2012]. O comissário biométrico é nomeado ao abrigo do *Code for Public Appointments* [código para as nomeações públicas] (o código está disponível na seguinte ligação: https://www.gov.uk/government/publications/governance-code-for-public-appointments) e as condições de nomeação deixam claro que o ministro da Administração Interna só pode ser destituído das suas funções em circunstâncias rigorosamente definidas, que incluem o incumprimento das suas obrigações durante um período de três meses, a condenação por infração penal ou o incumprimento das condições da sua nomeação.

([244]) O comissário para as câmaras de videovigilância foi criado pelo *Protection of Freedoms Act 2012* e tem a função de incentivar o cumprimento do *Surveillance Camera Code of Practice* (código de boas práticas sobre as câmaras de videovigilância); analisar o funcionamento deste código; e aconselhar os ministros sobre a necessidade de alteração deste código. O comissário é nomeado de acordo com as mesmas regras que os comissários biométricos e goza de poderes, recursos e proteção semelhantes contra a destituição.

([245]) Ver https://committees.parliament.uk/committee/83/home-affairs-committee/news/100537/work-of-the-national-crime-agency--scrutinised/

(165) No âmbito das suas competências, a comissão pode escolher o seu objeto de inquérito, incluindo casos específicos, desde que a questão não esteja *sub judice*. Pode ainda solicitar provas escritas e verbais de um vasto conjunto de grupos e pessoas singulares pertinentes. A comissão elabora relatórios sobre as suas conclusões e emite recomendações para o governo ([246]). Prevê-se que o governo responda a cada uma das recomendações do relatório no prazo de 60 dias ([247]).

(166) No domínio da vigilância, a comissão elaborou igualmente um relatório referente ao *Regulation of Investigatory Powers Act 2000* (RIPA 2000) ([248]), que concluiu que o RIPA 2000 não se adequava ao propósito. O relatório foi tido em conta durante a substituição de partes importantes do RIPA 2000 pelo IPA 2016. O sítio Web da comissão inclui uma lista completa dos inquéritos ([249]).

(167) As tarefas do HASC são realizadas na Escócia pelo Subcomité da Justiça para a Polícia e, na Irlanda do Norte, pelo Comité da Justiça ([250]).

3.2.4 *Recurso*

(168) No que se refere ao tratamento de dados pelas autoridades de aplicação da lei, a parte 3 do DPA 2018 e o IPA 2016, bem como o *Human Rights Act 1998*, preveem mecanismos de recurso.

(169) Este conjunto de mecanismos confere vias de recurso administrativas e judiciais eficazes aos titulares dos dados, o que lhes permite assegurar os seus direitos, nomeadamente o direito de acesso a dados pessoais que lhes digam respeito ou de obter a retificação ou a supressão desses dados.

(170) Em primeiro lugar, ao abrigo da *section 165* do DPA 2018, um titular dos dados tem o direito de apresentar reclamação ao comissário para a informação caso considere que existe uma violação da parte 3 do DPA 2018 no que diz respeito aos seus dados pessoais ([251]). O comissário para a informação tem o poder de avaliar o cumprimento do DPA 2018 do responsável pelo tratamento e do subcontratante, de exigir que estes tomem as medidas necessárias em caso de incumprimento e de impor coimas.

([246]) As comissões especiais, incluindo a *Home Affairs Select Committee*, estão sujeitas aos regulamentos da Câmara dos Comuns. Os regulamentos são as ordens, acordadas pela Câmara dos Comuns, que regulam a forma como o parlamento faz negócios. O âmbito das comissões especiais é amplo, sendo que o Regulamento 152, n.º 1, estabelece que «[a]s comissões especiais devem ser nomeadas por forma a analisar as despesas, a administração e a política dos principais departamentos governamentais, conforme enunciado no n.º 2, do presente regulamento e nos organismos públicos associados.» Tal habilita a *Home Affairs Select Committee* a analisar qualquer política detida pelo Ministério da Administração Interna, o que inclui as políticas (e a legislação conexa) em matéria de poderes de investigação. Além disso, o Regulamento 152, n.º 4, esclarece que as comissões têm diversos poderes, incluindo a capacidade de solicitar que as pessoas singulares apresentem provas ou documentos relativos a uma questão específica e de elaborar relatórios. Os inquéritos atuais e anteriores da comissão estão disponíveis na seguinte ligação https://committees.parliament.uk/committee/83/ /home-affairs-committee/

([247]) Os poderes da *Home Affairs Select Committee* em Inglaterra e no País de Gales estão estabelecidos nos regulamentos da Câmara dos Comuns, disponível na seguinte ligação: https://www.parliament.uk/business/publications/commons/standing-orders-public11/

([248]) Disponível na seguinte ligação: https://publications.parliament.uk/pa/cm201415/cmselect/cmhaff/711/71103.htm

([249]) Disponível na seguinte ligação: https://committees.parliament.uk/committee/83/home-affairs-committee

([250]) As regras do Subcomité da Justiça para a Polícia na Escócia são apresentadas na seguinte ligação https://www.parliament.scot/ /parliamentarybusiness/CurrentCommittees/justice-committee.aspx e as regras do Comité da Justiça na Irlanda do Norte são apresentadas na seguinte ligação: http://www.niassembly.gov.uk/assembly-business/standing-orders/

([251]) O último relatório anual do ICO apresenta uma distribuição da natureza das reclamações recebidas e encerradas. Em particular, o número de reclamações recebidas por «registos policiais e criminais» correspondem a 6% do número total de reclamações recebidas (com um aumento de 1% comparativamente ao exercício financeiro anterior). O relatório anual revela igualmente que as reclamações que dizem respeito aos pedidos de acesso dos titulares representam o número mais elevado (46% do número total de reclamações, com um aumento de 8% comparativamente ao exercício financeiro anterior) (relatório anual do ICO de 2019-2020, p. 55; ver a nota de rodapé 88).

(171) Em segundo lugar, o DPA 2018 prevê o direito à ação judicial contra o comissário para a informação se este não tratar adequadamente uma reclamação efetuada pelo titular de dados. Mais especificamente, caso o comissário não der «andamento» ([252]) a uma reclamação efetuada pelo titular de dados, o autor da reclamação tem acesso à ação judicial, uma vez que pode recorrer a um tribunal de primeira instância ([253]) para ordenar que o comissário tome as medidas adequadas para dar resposta à reclamação ou informe o autor da reclamação do andamento da reclamação ([254]). Além disso, qualquer pessoa que receba uma das notificações mencionadas (notificações informativas, de avaliação, de execução ou de sanção) emitidas pelo comissário pode recorrer a um tribunal de primeira instância. Se o tribunal considerar que a decisão do comissário não respeita a lei ou que o comissário para a informação deveria ter exercido o seu critério de outra forma, o tribunal deve permitir o recurso ou substituir outra notificação ou decisão que poderia ter sido emitida ou dada pelo comissário para a informação ([255]).

(172) Em terceiro lugar, as pessoas singulares podem obter o direito ao recurso judicial contra um responsável pelo tratamento ou um subcontratante diretamente nos tribunais. Em particular, ao abrigo da *section 167* do DPA 2018, um titular de dados pode interpor uma ação no tribunal por uma violação dos direitos que lhe são conferidos ao abrigo da legislação em matéria de proteção de dados e o tribunal pode solicitar que o responsável pelo tratamento tome (ou se abstenha de tomar) medidas relativas ao tratamento para cumprir o DPA 2018, por meio de uma ordem. Além disso, ao abrigo da *section 169* do DPA 2018, qualquer pessoa que tenha sofrido danos devido a uma violação de um requisito da legislação em matéria de proteção de dados (incluindo a parte 3 do DPA 2018), que não seja o RGPD do Reino Unido, tem direito a indemnização por esses danos do responsável pelo tratamento ou do subcontratante, salvo se o mesmo conseguir provar que não é de modo algum responsável pelo evento que deu origem aos danos. Os danos incluem perdas financeiras e não financeiras, como sofrimento emocional.

(173) Por último, qualquer pessoa que considere que os direitos que lhes são conferidos foram violados, incluindo o direito à privacidade e à proteção dos dados, por alguma autoridade pública, podem obter reparação dos tribunais do Reino Unido ao abrigo do *Human Rights Act 1998* ([256]), e, depois de esgotadas as vias de recurso nacionais, as pessoas singulares, as organizações não governamentais e os grupos de pessoas singulares podem obter vias de recurso junto do Tribunal Europeu dos Direitos Humanos por violações dos direitos consagrados na Convenção Europeia dos Direitos Humanos ([257]) (ver o considerando 111).

3.2.4.1 Mecanismos de recurso previstos no IPA 2016

(174) As pessoas singulares podem obter reparação por violações do IPA 2016 junto do *Investigatory Powers Tribunal* (Tribunal de Instrução). As vias de recurso previstas no IPA 2016 são descritas nos considerandos 263 a 269) .

([252]) A *section 166* do DPA 2018 diz respeito especificamente às seguintes situações: a) o comissário não toma as medidas adequadas para dar resposta à reclamação, b) o comissário não informa o autor da reclamação do andamento ou do resultado da reclamação antes do final do prazo de três meses que tem início quando o comissário recebeu a reclamação ou c) se a análise da reclamação efetuada pelo comissário não for concluída dentro desse prazo e se o comissário não fornecer essas informações ao autor da reclamação num prazo subsequente de três meses.

([253]) O *First-tier Tribunal* é o tribunal competente para o tratamento de recursos contra as decisões tomadas pelos organismos regulamentares do governo. No caso da decisão do comissário para a informação, a secção competente é a «General Regulatory Chamber», que tem jurisdição em todo o Reino Unido.

([254]) *Section 166* do DPA 2018. Os exemplos de ações judiciais de sucesso contra o ICO incluem um caso em que o ICO reconheceu a receção de uma reclamação de um titular de dados, mas não indicou quais as medidas que iria tomar e, como tal, foi ordenado que confirmasse, no prazo de 21 dias úteis, se iria investigar as reclamações e, em caso afirmativo, que informasse o autor da reclamação do andamento da investigação com uma frequência não inferior a 21 dias úteis (o acórdão ainda não foi publicado) e um caso em que o First-tier Tribunal considerou que não era claro se a resposta do ICO a um autor da reclamação constituía adequadamente o «resultado» da reclamação (ver Susan Milne/Information Commissioner [2020], acórdão disponível na seguinte ligação: https://informationrights.decisions.tribunals.gov.uk/DBFiles/Decision/i2730/Milne,%20S%20-%20QJ2020-0296-GDPR-V,%20051220%20Section%20166%20DPA%20-DECISION.pdf).

([255]) *Sections 162* e *163* do DPA 2018.

([256]) Ver, por exemplo, *Brown/Commissioner of Police of the Metropolis & Anor* [2019] EWCA Civ 1724 em que, ao abrigo do DPA 1998 e do *Human Rights Act 1998*, foi determinada uma indemnização no valor de 9 000 GBP pela obtenção ilícita e pela utilização indevida de dados pessoais e *R (on the application of Bridges)/Chief Constable of South Wales* [2020] EWCA Civ 1058, em que o *Court of Appeal* declarou ilícita a aplicação de um sistema de reconhecimento facial pela polícia do País de Gales, uma vez que tal violava o artigo 8.º da CEDH e a avaliação do impacto sobre a proteção de dados elaborada pelo responsável pelo tratamento não cumpria o DPA 2018.

([257]) O artigo 34.º da Convenção Europeia dos Direitos Humanos determina que «[o] tribunal pode receber ações judiciais de qualquer pessoa singular, organização não governamental ou grupo de pessoas singulares que reclame ser vítima de uma violação dos direitos consagrados na Convenção ou nos Protocolos por parte de uma das altas partes contratantes. As altas partes contratantes comprometem-se a não prejudicar o exercício efetivo deste direito».

3.3 **Acesso e utilização pelas autoridades públicas do Reino Unido para efeitos de segurança nacional**

(175) Na ordem jurídica do Reino Unido, os serviços de informações com competência para recolher informações eletrónicas na posse de responsáveis pelo tratamento ou subcontratantes por razões de segurança nacional, em situações pertinentes para um cenário de adequação, são o serviço de segurança ([258]) (MI5), o serviço de informações secretas ([259]) (SIS) e a sede de comunicações governamentais ([260]) (GCHQ) ([261]).

3.3.1 *Bases jurídicas, limitações e garantias*

(176) No Reino Unido, os poderes das agências de informações encontram-se estabelecidos no IPA 2016 e no RIPA 2000, que, em conjunto com o DPA 2018, definem o âmbito material e pessoal destes poderes, bem como as restrições e as garantias para o seu exercício. Esses poderes, bem como as limitações e as garantias aplicáveis aos mesmos, são avaliadas pormenorizadamente nas secções seguintes.

3.3.1.1 Poderes de investigação exercidos no contexto da segurança nacional

(177) O IPA 2016 apresenta o quadro jurídico para a utilização dos poderes de investigação, ou seja, o poder de intercetar, aceder aos dados de comunicações e de realizar interferências com os equipamentos. O IPA 2016 introduz uma proibição geral e criminaliza a utilização de técnicas que permitem o acesso aos conteúdos das comunicações, o acesso aos dados de comunicações ou interferências com os equipamentos caso não seja uma autoridade legítima ([262]). Isto reflete-se no facto de a utilização destes poderes de investigação apenas ser legítima nos casos em que é efetuada com recurso a um mandado ou autorização ([263]).

(178) O IPA 2016 estabelece regras pormenorizadas que regem o âmbito e a aplicação de cada um dos poderes de investigação, bem como as respetivas restrições e garantias específicas. Aplicam-se diferentes regras dependendo do tipo de poder de investigação (interceção de comunicações, aquisição e conservação de dados

([258]) O MI5 é a autoridade do ministro da Administração Interna. O *Security Service Act 1989* estabelece as funções do MI5: proteger a segurança nacional (incluindo a proteção contra ameaças de espionagem, terrorismo e sabotagem, contra atividades de agentes de potências estrangeiras e de ações que visam opor-se ou prejudicar a democracia parlamentar através de ações políticas, industriais ou violentas), proteger o bem-estar económico do Reino Unido contra ameaças externas e apoiar atividades das forças policiais e de outras agências de aplicação da lei na prevenção e deteção da criminalidade grave.

([259]) O SIS está sob a alçada do ministro dos Negócios Estrangeiros e as suas funções encontram-se estabelecidas no *Intelligence Services Act 1994*. As suas funções passam por obter e prestar informações sobre as ações ou as intenções das pessoas que não habitam nas Ilhas Britânicas e realizar outras tarefas relativas às ações ou intenções dessas pessoas. Essas funções apenas podem ser exercidas no interesse da segurança nacional, no interesse do bem-estar económico do Reino Unido ou para apoiar a prevenção e a deteção da criminalidade grave.

([260]) O GCHQ está sob a alçada do ministro dos Negócios Estrangeiros e as suas funções encontram-se estabelecidas no *Intelligence Services Act 1994*. Estas funções incluem a) controlar, utilizar ou interferir com as emissões eletromagnéticas e de outro tipo e com os equipamentos que produzem essas emissões, obter e prestar informações resultantes de ou relacionadas com essas emissões ou equipamentos e de materiais encriptados; b) aconselhar e prestar assistência linguística, incluindo a terminologia utilizada para questões técnicas e criptografia e outras questões relacionadas com a proteção das informações para as forças armadas, o governo ou outras organizações ou pessoas consideradas adequadas. Essas funções apenas podem ser exercidas no interesse da segurança nacional, no interesse do bem-estar económico do Reino Unido relativamente às ações ou intenções das pessoas que não habitam nas Ilhas Britânicas ou para apoiar a prevenção ou a deteção da criminalidade grave.

([261]) Outros organismos públicos que exercem funções relevantes para a segurança nacional são o *Defence Intelligence* (DI), o *National Security Council and Secretariat*, o *Joint Intelligence Organisation* e o *Joint Intelligence Committee*. Contudo, nem o *Joint Intelligence Committee* nem o *Joint Intelligence Organisation*, podem utilizar os poderes de investigação ao abrigo do IPA 2016 enquanto o DI tem um âmbito limitado para a utilização dos seus poderes.

([262]) A proibição aplica-se às redes de comunicações públicas e privadas, bem como ao serviço postal público quando a interceção é realizada no Reino Unido. A proibição não se aplica ao responsável pelo tratamento da rede particular caso o mesmo tenha dado o consentimento expresso ou implícito para a realização da interceção (*section 3* do IPA 2016).

([263]) Em casos específicos e limitados, é possível efetuar uma interceção lícita sem um mandado, ou seja, quando a interceção é realizada com o consentimento do remetente ou do destinatário (*section 44* do IPA 2016), em caso de finalidades administrativas ou de execução limitadas (*sections 45* a *48* do IPA), em determinadas instituições especiais (*sections 49* a *51* do IPA 2016) e de acordo com os pedidos do estrangeiro (*section 52* do IPA 2016).

de comunicações e interferência com os equipamentos) e dependendo se o poder é exercido num grupo-alvo específico ([264]) ou em larga escala. Os pormenores sobre o âmbito, as garantias e as restrições de cada medida prevista pelo IPA 2016 encontram-se descritos na secção específica abaixo.

(179) Além disso, o IPA 2016 é complementado por um conjunto de códigos de boas práticas, emitidos pelo ministro da tutela, aprovados pelas câmaras do parlamento ([265]) e aplicáveis no país, que fornecem orientações adicionais para a utilização destes poderes ([266]). Embora os titulares dos dados possam recorrer diretamente às disposições estabelecidas no IPA 2016 a fim de exercerem os seus direitos, o *schedule 7*, n.º 5, do IPA 2016, especifica que os códigos de boas práticas são admissíveis como provas em processos cíveis e penais, e o tribunal ou a autoridade de controlo pode ter em conta qualquer incumprimento dos códigos ao determinar uma questão pertinente em processos judiciais ([267]). No contexto da sua avaliação da «qualidade do direito» da legislação anterior do Reino Unido no domínio da vigilância, o RIPA 2000, a Grande Secção do Tribunal Europeu dos Direitos Humanos reconheceu expressamente a pertinência dos códigos de boas práticas do Reino Unido e aceitou que as respetivas disposições fossem tidas em conta na avaliação da previsibilidade da legislação que permite a vigilância ([268]).

(180) Importa salientar, portanto, que os poderes direcionados (interceção direcionada ([269]), aquisição de dados de comunicações ([270]), conservação de dados de comunicações ([271]) e interferência específica com os equipamentos ([272])) são disponibilizados às agências de segurança nacionais e a determinadas autoridades de aplicação da lei ([273]), ao passo que apenas os serviços de informações podem utilizar os poderes em larga escala (ou seja, interceção em larga escala ([274]), aquisição em larga escala de dados de comunicações ([275]), interferência com os equipamentos em larga escala ([276]) e conjuntos de dados pessoais em larga escala ([277])).

(181) Ao decidir qual dos poderes de investigação deve ser utilizado, a agência de informações deve cumprir os «deveres gerais relativos à privacidade» enumerados na *section 2(2)(a)* do IPA 2016, que inclui um teste de necessidade e proporcionalidade. Mais especificamente, nos termos desta disposição, uma autoridade pública que tenha a intenção de utilizar um poder de investigação deve considerar i) se é possível obter a mesma coisa que se pretende obter com o mandado, a autorização ou a notificação através de outros meios menos intrusivos; ii) se o nível de

([264]) No que diz respeito, por exemplo, ao âmbito de tais medidas, nas partes 3 e 4 (conservação e aquisição de dados de comunicação), o âmbito da medida está estreitamente associado à definição de «operadores de telecomunicações», cujos dados dos utilizadores estão sujeitos à medida. Pode ser apresentado outro exemplo em relação à utilização de poderes «em larga escala». Neste caso, o âmbito destes poderes limita-se às «comunicações enviadas ou recebidas por pessoas singulares que se encontram fora das ilhas Britânicas».

([265]) O *schedule 7* do IPA 2016 determina o âmbito de aplicação dos códigos, o procedimento a seguir para a sua emissão, as regras para a respetiva revisão e o efeito dos códigos.

([266]) Os códigos de boas práticas previstos no IPA 2016 estão disponíveis na seguinte ligação: https://www.gov.uk/government/publications/investigatory-powers-act-2016-codes-of-practice

([267]) Os tribunais recorrem aos códigos de boas práticas para avaliar a legitimidade da conduta das autoridades. Ver, por exemplo: *Dias/Cleveland Police*, [2017] UKIPTrib15_586-CH, em que o *Investigatory Powers Tribunal* fez referência a passagens específicas do código de boas práticas sobre os dados de comunicações para compreender a definição das razões de «prevenção ou deteção da criminalidade ou a defesa da ordem» utilizada para aplicar a aquisição de dados de comunicações. O código foi incluído na fundamentação utilizada para determinar se essa razão foi utilizada incorretamente. O tribunal concluiu que as condutas contestadas eram ilícitas. Os tribunais efetuaram igualmente a avaliação do nível de garantias disponíveis nos códigos, ver, por exemplo, *Just for Law Kids/Secretary of State for the Home Department* [2019] EWHC 1772 (Admin), no qual o *High Court* constatou que, a legislação primária e secundária, em conjunto com as orientações internas, concediam garantias suficientes; ou *R (National Council for Civil Liberties)/Secretary of State for the Home Department e o.* [2019] EWHC 2057 (Admin), em que se concluiu que o IPA 2016 e o *Code of Practice on Equipment Interference* incluíam disposições suficientes quanto à necessidade de mandados específicos.

([268]) No processo *Big Brother Watch*, a Grande Secção do Tribunal Europeu dos Direitos Humanos observou que «o código do comissário para a informação é um documento público aprovado por ambas as câmaras do parlamento, publicado pelo Governo em linha e em versão impressa, e deve ser tido em conta tanto pelas pessoas que exercem funções de interceção como pelos tribunais (ver os n.os 93 e 94 acima). Consequentemente, este tribunal admitiu que as respetivas disposições fossem tidas em conta na avaliação da previsibilidade do RIPA (ver *Kennedy*, supramencionado, § 157). Em conformidade, o tribunal admitiria que o direito interno fosse adequadamente «acessível» (ver Tribunal Europeu dos Direitos Humanos (Grande Secção), *Big Brother Watch e o./Reino Unido*, pedidos n.os 58170/13, 62322/14 e 24960/15, de 25 de maio de 2021, n.º 366).

([269]) Parte 2 do IPA 2016.

([270]) Parte 3 do IPA 2016.

([271]) Parte 4 do IPA 2016.

([272]) Parte 5 do IPA 2016.

([273]) Para consultar a lista de autoridades de aplicação da lei competentes que podem aplicar os poderes de investigação direcionados ao abrigo do IPA 2016, ver a nota de rodapé 139.

([274]) *Section 136* do IPA 2016.

([275]) *Section 158* do IPA 2016.

([276]) *Section 176* do IPA 2016.

([277]) *Section 199* do IPA 2016.

proteção a aplicar relativamente à obtenção de informações através do mandado, da autorização ou da notificação é superior por causa da sensibilidade particular dessa informação; iii) o interesse público na integridade e na segurança dos sistemas de telecomunicações e dos serviços postais; e iv) quaisquer outros aspetos de interesse público na proteção da privacidade ([278]).

(182) A forma como estes critérios devem ser aplicados — e a forma como o seu cumprimento é avaliado no âmbito da autorização da utilização desses poderes pelo ministro da tutela e os comissários judiciais independentes — é especificada em maior detalhe nos códigos de boas práticas pertinentes. Em particular, a utilização de algum destes poderes de investigação deve ser sempre «proporcional aos objetivos pretendidos, o [que] implica equilibrar a gravidade da intrusão na privacidade [e outras considerações estabelecidas na *section 2(2)*] tendo em conta a necessidade da atividade em termos investigativos, operacionais ou de capacidade». Isto significa que «deve oferecer uma perspetiva realista e conferir os benefícios esperados e não deve ser desproporcionado ou arbitrário» e «[nenh] uma interferência com a privacidade deve ser considerada proporcionada caso as informações que se procura obter possam ser razoavelmente obtidas através de outros meios menos intrusivos» ([279]). Mais especificamente, o cumprimento do princípio de proporcionalidade deve ser avaliado tendo em conta os seguintes critérios: «i) a medida da interferência com a privacidade proposta tendo em conta os objetivos pretendidos; ii) como e por que motivo os métodos que serão adotados causarão a menor interferência possível à pessoa em causa e aos outros; iii) se a atividade é uma utilização adequada da lei e uma forma razoável de atingir os objetivos pretendidos, depois de ponderadas todas as alternativas razoáveis; iv) que outros métodos, conforme apropriados, não foram implementados ou, tendo sido implementados, foram avaliados como insuficientes para alcançarem os objetivos operacionais sem a utilização do poder de investigação proposto» ([280]).

(183) Na prática, conforme explicado pelas autoridades do Reino Unido, isto assegura que, em primeiro lugar, uma agência de informações define o objetivo operacional (delimitando assim a recolha, por exemplo, uma finalidade de combater o terrorismo internacional numa zona geográfica específica) e, em segundo lugar, com base nesse objetivo operacional, terá de ponderar qual a opção técnica (por exemplo, interceção direcionada ou em larga escala, interferência com os equipamentos, aquisição de dados de comunicações) é a mais proporcionada [ou seja, o meio menos intrusivo para a privacidade; ver a *section 2(2)* do IPA] tendo em conta os objetivos pretendidos e, como tal, pode ser autorizada numa das bases legais disponíveis.

(184) Importa salientar que este recurso às normas de necessidade e proporcionalidade foi destacado e acolhido com agrado pelo relator especial da ONU sobre o direito à privacidade, Joseph Cannataci, o qual declarou, relativamente ao sistema criado pelo IPA 2016, que «[o]s procedimentos instaurados nos serviços de informações e nas agências de aplicação da lei parecem necessitar sistematicamente de ter em conta a necessidade e a proporcionalidade de uma medida ou operação de vigilância antes de a sua autorização ser recomendada, bem como antes de ser revista pelos mesmos motivos» ([281]). Ele observou igualmente que na sua reunião com os representantes das agências de aplicação da lei e de segurança nacional «[ele] recebeu um consenso de que o direito à privacidade necessita de ser uma consideração principal em qualquer decisão relativa a medidas de vigilância. Todos eles compreenderam e apreciaram a necessidade e a proporcionalidade como princípios essenciais a ter em conta».

([278]) O *Code of Practice on Interception of Communications* (código de boas práticas sobre a interceção das comunicações) especifica que outros elementos do teste de proporcionalidade são: «i) a medida da interferência com a privacidade proposta tendo em conta os objetivos pretendidos; ii) como e por que motivo os métodos que serão adotados causarão a menor interferência possível à pessoa em causa e aos outros; iii) se a atividade é uma utilização adequada da lei e uma forma razoável de atingir os objetivos pretendidos, depois de ponderadas todas as alternativas razoáveis; iv) que outros métodos, conforme apropriados, não foram implementados ou, tendo sido implementados, foram avaliados como insuficientes para alcançarem os objetivos operacionais sem a utilização do poder de investigação proposto». *Code of Practice on Interception of Communications*, ponto 4.16, disponível na seguinte ligação: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715480/Interception_of_Communications_Code_of_Practice.pdf

([279]) Ver *Code of Practice on Interception of Communications*, pontos 4.12 e 4.15, disponível na seguinte ligação: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715480/Interception_of_Communications_Code_of_Practice.pdf

([280]) Ver *Code of Practice on Interception of Communications*, ponto 4.16.

([281]) *End of Mission Statement of the Special Rapporteur on the Right to Privacy at the Conclusion Of his Mission to the United Kingdom of Great Britain and Northern Ireland* (Declaração de fim de missão do relator especial da ONU sobre o direito à privacidade na conclusão da sua missão para o Reino Unido da Grã-Bretanha e da Irlanda do Norte), disponível na seguinte ligação: https://www.ohchr.org/EN//NewsEvents/Pages/DisplayNews.aspx?NewsID=23296&LangID=E, n.º 1.a.

(185) Os critérios específicos para emitir os diferentes mandados, bem como as limitações e as garantias criadas pelo IPA 2016 relativas a cada poder de investigação são descritas em maior detalhe nos considerandos 186 a 243.

3.3.1.1.1 Interceção e exame direcionados

(186) Existem três tipos de mandado para interceções direcionadas: o mandado de interceção direcionada ([282]), o mandado de exame direcionado e um mandado de assistência mútua ([283]). As condições para obter tais mandados, bem como as garantias aplicáveis estão previstas na parte 2, capítulo 1, do IPA 2016.

(187) Um mandado de interceção direcionada autoriza a interceção das comunicações descritas no mandado no decurso da sua transmissão e a obtenção de outros dados pertinentes para essas comunicações ([284]), incluindo dados secundários ([285]). Um mandado de exame direcionado autoriza uma pessoa a efetuar a seleção para exame do conteúdo intercetado obtido ao abrigo de um mandado de interceção em larga escala ([286]).

(188) Qualquer mandado nos termos da Parte 2 do IPA 2016 pode ser emitido pelo ministro da tutela ([287]) e aprovado por um comissário judicial ([288]). Em todos os casos, a duração de qualquer tipo de mandado direcionado é limitada a seis meses ([289]) e aplicam-se regras específicas relativas à sua alteração ([290]) e renovação ([291]).

(189) Antes de emitir o mandado, o ministro da tutela deve proceder a uma avaliação da necessidade e da proporcionalidade ([292]). Especificamente, para um mandado de interceção direcionada e um mandado de exame direcionado, o ministro da tutela deve verificar se a medida é necessária por um dos seguintes motivos: interesse da segurança nacional, prevenção ou deteção da criminalidade grave, ou o interesse do bem-estar económico do Reino Unido ([293]), na medida em que esse interesse seja igualmente relevante para o interesse da segurança nacional ([294]). Por outro lado, um mandado de assistência mútua (ver o considerando 139 acima) só pode ser emitido se o ministro da tutela considerar que existem circunstâncias equivalentes àquelas em que emitiria um mandado para efeitos de prevenção e/ou deteção da criminalidade grave ([295]).

(190) Além disso, o ministro da tutela deve apreciar se a medida é proporcional ao que se pretende alcançar ([296]). A apreciação da proporcionalidade das medidas solicitadas deve ter em conta os deveres gerais em matéria de privacidade previstos na *section 2(2)* do IPA 2016, nomeadamente a necessidade de apreciar se o que se pretende alcançar através do mandado, da autorização ou da notificação pode ser razoavelmente alcançado por outros meios

([282]) *Section 15(2)* do IPA 2016.
([283]) *Section 15(4)* do IPA 2016.
([284]) *Section 15(2)* do IPA 2016.
([285]) Os dados secundários são dados anexos ou logicamente associados à comunicação intercetada, podendo estar logicamente separados da mesma e, se assim for, não revelando nada do que se poderia razoavelmente considerar ser o significado (se for caso disso) da comunicação. Alguns exemplos de dados secundários incluem configurações do encaminhador ou das barreiras de segurança, ou o período de tempo em que um encaminhador esteve ativo numa rede quando estes fazem parte, estão ligados ou estão logicamente associados à comunicação intercetada. Para mais informações, ver a definição constante da *section 16* do IPA 2016 e o *Code of Practice on Interception of Communications*, ponto 2.19, ver a nota de rodapé 278.
([286]) Este exame é efetuado como exceção ao disposto na *section 152(4)* do IPA 2016, que prevê a proibição de procurar identificar a comunicação de pessoas que se encontrem nas ilhas Britânicas. Ver o considerando 229.
([287]) O ministro escocês autoriza o mandado quando este diz respeito a atividades criminosas graves na Escócia (ver a *section 21* e a *section 22* do IPA 2016), ao passo que o ministro da tutela pode designar um dirigente superior para emitir um mandado de assistência mútua quando se afigure que a interceção dirá respeito a uma pessoa ou instalações localizadas fora do Reino Unido (*section 40* do IPA 2016).
([288]) *Sections 19* e *23* do IPA 2016.
([289]) *Section 32* do IPA 2016.
([290]) *Section 39* do IPA 2016. Pessoas especificamente indicadas podem introduzir alterações limitadas nos mandados, ao abrigo das condições estabelecidas no IPA 2016. A pessoa que emitiu o mandado pode anular um mandado a qualquer momento. Deve fazê-lo se o mandado já não for necessário por qualquer razão pertinente ou se a conduta autorizada pelo mandado deixar de ser proporcional ao que se pretende alcançar.
([291]) *Section 33* do IPA 2016. A decisão de renovação do mandado deve ser aprovada por um comissário judicial.
([292]) *Section 19* do IPA 2016.
([293]) Quanto ao conceito de «interesse do bem-estar económico do Reino Unido, na medida em que esse interesse seja igualmente relevante para a segurança nacional», a Grande Secção do Tribunal Europeu dos Direitos Humanos considerou, no acórdão *Big Brother Watch e o./Reino Unido* (ver a nota de rodapé 268 acima), n.º 371, que este conceito se encontrava suficientemente centrado na segurança nacional. Embora a conclusão do tribunal neste processo estivesse relacionada com a utilização desta noção no RIPA 2000, a mesma noção é utilizada no IPA 2016.
([294]) *Section 20(2)* do IPA 2016.
([295]) *Section 20(3)* do IPA 2016.
([296]) *Sections 19(1)(b)*, *19(2)(b)* e *19(3)(b)* do IPA 2016.

menos intrusivos e se o nível de proteção a aplicar em relação a qualquer obtenção de informações, por força do mandado, é mais elevado devido à natureza particularmente sensível dessas informações (ver o considerando 181 acima).

(191) Para o efeito, o ministro da tutela terá de ter em conta todos os elementos do pedido apresentados pela autoridade que o apresenta, em especial os relacionados com as pessoas a intercetar e a relevância da medida para a investigação. Tais elementos estão descritos no *Code of Practice on Interception of Communications* e devem ser descritos com um certo grau de especificidade ([297]). Além disso, a section 17 do IPA 2016 exige que qualquer mandado emitido ao abrigo do capítulo 2 da mesma lei designe ou descreva a pessoa ou o grupo de pessoas, a organização ou instalações a intercetar («alvo»). No caso de um mandado de interceção direcionada ou de um mandado de exame direcionado, estes podem também dizer respeito a um grupo de pessoas, a mais do que uma pessoa ou organização, ou a mais do que um conjunto de instalações (também designado por «mandado temático») ([298]). Nestes casos, o mandado deve descrever o objetivo comum ou a atividade partilhada pelo grupo de pessoas ou a operação/ /investigação e designar ou descrever tantas pessoas/organizações ou conjuntos de instalações quanto possível, quando tal se mostre razoavelmente exequível ([299]). Por último, todos os mandados emitidos ao abrigo da parte 2 do IPA 2016 devem especificar os endereços, números, aparelhos, fatores ou combinação de fatores que devem ser utilizados para identificar as comunicações ([300]). A este respeito, o *Code of Practice on Interception of Communications* especifica que, no caso de um mandado de interceção direcionada e de um exame orientado, «o mandado deve especificar (ou descrever) os fatores ou a combinação de fatores que devem ser utilizados para identificar as comunicações. Sempre que as comunicações devam ser identificadas por referência a um número de telefone (por exemplo), o número deve ser especificado através da sua comunicação na íntegra. No entanto, sempre que se pretenda utilizar seletores de Internet muito complexos ou em constante mudança para identificar as comunicações, esses seletores devem ser descritos tanto quanto possível» ([301]).

(192) Uma garantia importante neste contexto é que a avaliação efetuada pelo ministro da tutela para emitir um mandado deve ser aprovada por um comissário judicial ([302]) independente que verificará, nomeadamente, se a decisão de emitir o mandado respeita os princípios da necessidade e da proporcionalidade ([303]) (sobre o estatuto e o papel dos comissários judiciais ver os considerandos 251 a 256 abaixo). O IPA 2016 esclarece igualmente que, ao proceder a essa verificação, o comissário judicial deve aplicar os mesmos princípios que os aplicados por um tribunal a um pedido de exame judiciário ([304]). Deste modo garante-se, em cada caso e antes do acesso aos dados, a verificação sistemática do cumprimento dos princípios da necessidade e da proporcionalidade por um organismo independente.

(193) O IPA 2016 prevê poucas exceções específicas e limitadas para a realização de interceções direcionadas sem um mandado. Os casos limitados encontram-se especificados na lei ([305]) e, com exceção do que se baseia no «consentimento» do remetente/destinatário, são executadas por pessoas (organismos públicos ou privados) diferentes das agências de segurança nacional. Além disso, este tipo de interceção é efetuado para efeitos diferentes da recolha de «informações» ([306]) e, em alguns casos, é muito improvável que a recolha possa ocorrer no contexto de um cenário de «transferência» (por exemplo, em caso de interceção efetuada num hospital psiquiátrico ou numa

([297]) As informações solicitadas incluem informações pormenorizadas sobre os antecedentes (descrição das pessoas/organizações/ /conjunto de instalações, comunicação a intercetar) e a forma como a obtenção dessas informações será benéfica para a investigação, bem como uma descrição da conduta a autorizar. Caso não seja possível descrever as pessoas/organizações/instalações, deve incluir-se uma explicação sobre a razão pela qual não foi possível ou sobre a razão pela qual apenas se efetuou uma descrição geral (*Code of Practice on Interception of Communications*, pontos 5.32 e 5.34, ver a nota de rodapé 278).

([298]) *Section 17(2)* do IPA 2016. Ver também o *Code of Practice on Interception of Communications* (código de boas práticas sobre a interceção das comunicações), pontos 5.11 e seguintes, ver a nota de rodapé 278.

([299]) *Section 31(4)* e *(5)* do IPA 2016.

([300]) *Section 31(8)* do IPA 2016.

([301]) *Code of Practice on Interception of Communications*, pontos 5.37 e 5.38, ver a nota de rodapé 278.

([302]) A aprovação por um comissário judicial não é necessária quando o ministro da tutela considerar que existe uma necessidade urgente de emitir o mandado [*section 19(1)* do IPA]. No entanto, o comissário judicial deve ser informado num curto espaço de tempo e decidir se aprova ou não o mandado. Caso contrário, o mandado deixa de produzir efeitos (*sections 24* e *25* do IPA 2016).

([303]) *Section 23(1)* do IPA 2016.

([304]) *Section 23(2)* do IPA 2016.

([305]) Ver *sections 44* a *51* do IPA 2016 e *section 12* do código de boas práticas da sobre a interceção das comunicações (ver a nota de rodapé 278).

([306]) É o caso, por exemplo, quando é necessária uma interceção numa prisão ou num hospital psiquiátrico (a fim de verificar a conduta de uma pessoa detida ou de um paciente) ou por um operador postal ou de telecomunicações, por exemplo, a fim de detetar conteúdos abusivos.

prisão). Tendo em conta a natureza do organismo a que estes casos específicos são aplicáveis (diferentes das agências de segurança nacional), serão aplicáveis todas as garantias previstas na parte 2 do DPA 2018 e no RGPD do Reino Unido, incluindo a supervisão do ICO e os mecanismos de recurso disponíveis. Além disso, para além das garantias previstas no DPA 2018, em determinados casos, o IPA 2016 prevê igualmente a supervisão *ex post* do IPCO ([307]).

(194) Quando a interceção é efetuada, são aplicáveis restrições e garantias adicionais, tendo em conta o estatuto específico das pessoas intercetadas ([308]). Por exemplo, a interceção de elementos sujeitos à prerrogativa legal de confidencialidade só é autorizada em caso de circunstâncias excecionais e imperiosas; a pessoa que emite o mandado deve ter em conta o interesse público na confidencialidade dos elementos sujeitos à prerrogativa legal de confidencialidade e a existência de requisitos específicos para o tratamento, conservação e divulgação desse material ([309]).

(195) Além disso, o IPA 2016 prevê salvaguardas específicas em matéria de segurança, conservação e divulgação que o ministro da tutela deve ter em conta antes de emitir um mandado específico ([310]). Em especial, a *section 53(5)* do IPA 2016 exige que todas as cópias de qualquer material recolhido ao abrigo do mandado sejam armazenadas de forma segura e destruídas logo que deixem de existir motivos pertinentes para a sua conservação, ao passo que a *section 53(2)* do IPA 2016 exige que o número de pessoas a quem o material é divulgado e em que medida qualquer material é divulgado, disponibilizado ou copiado deve ser limitado ao mínimo necessário para as finalidades legais.

(196) Por último, quando o material intercetado por um mandado de interceção direcionada ou por um mandado de assistência mútua deva ser entregue a um país terceiro («divulgações no estrangeiro»), o IPA 2016 prevê que o ministro da tutela deve assegurar a implementação de mecanismos adequados para garantir a existência de salvaguardas semelhantes em matéria de segurança, conservação e divulgação nesse país terceiro ([311]). Além disso a *section 109(2)* do DPA 2018 prevê que os serviços de informações só possam transferir dados pessoais fora do território do Reino Unido se a transferência for uma medida necessária e proporcionada efetuada para efeitos das funções legais do responsável pelo tratamento ou para outras finalidades previstas na *section 2(2)(a)* do *Security Service Act 1989* ou nas *sections 2(2)(a)* e *4(2)(a)* do *Intelligence Services Act 1994* ([312]). Importa notar que estes requisitos são igualmente aplicáveis nos casos em que é invocada a isenção relativa à segurança nacional nos termos da *section 110* do DPA 2018, uma vez que a *section 110* do DPA de 2018 não enumera a *section 109* do DPA 2018 como uma das disposições que não são suscetíveis de aplicação se for necessária uma isenção de determinadas disposições para efeitos de garantia da segurança nacional.

3.3.1.1.2 Aquisição e conservação direcionadas de dados de comunicações

(197) O IPA 2016 permite que o ministro da tutela imponha aos operadores de telecomunicações a conservação dos dados de comunicações para efeitos do acesso específico por parte de uma série de autoridades públicas, incluindo os serviços responsáveis pela aplicação da lei e os serviços de informações. A parte 4 do 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 do IPA 2016, estabelecem-se igualmente limitações específicas à utilização destes poderes e preveem salvaguardas específicas.

([307]) Ver, *a contrario*, *section 229(4)* do IPA.

([308]) As *sections 26* a *29* do IPA 2016 introduzem limitações à obtenção de mandados de interceção e exame direcionados relacionados com a interceção de comunicações enviadas por uma pessoa que seja deputado ao parlamento (qualquer parlamento do Reino Unido) ou as destinadas a este, a interceção de elementos sujeitos à prerrogativa legal de confidencialidade, a interceção de comunicações que a autoridade intercetora considere serem comunicações que contêm material jornalístico confidencial e quando o objetivo do mandado for identificar ou confirmar uma fonte de informação jornalística.

([309]) *Section 26* do IPA 2016.

([310]) *Section 19(1)* do IPA 2016.

([311]) *Section 54* do IPA 2016. As garantias relativas à divulgação de material a autoridades estrangeiras são especificadas mais pormenorizadamente nos códigos de boas práticas: ver, em especial, os n.os 9.26 e seguintes e o n.º 9.87 do *Code of Practice on the Interception of Communications* e os n.os 9.33 e seguintes e o n.º 9.41 do *Code of Practice on Equipment Interference* (ver a nota de rodapé 278).

([312]) Estas finalidades são: relativamente ao serviço de segurança, a prevenção ou deteção da criminalidade grave ou quaisquer processos penais [*section 2(2)(a)* do *Security Service Act 1989*], relativamente ao serviço de informações, o interesse da segurança nacional, a prevenção ou deteção da criminalidade grave ou quaisquer processos penais [*section 2(2)(a)* do *Intelligence Services Act 1994*], e relativamente ao GCHQ, quaisquer processos penais [*section 4(2)(a)* do *Intelligence Services Act 1994*]. Ver igualmente *Explanatory notes* sobre o DPA 2018, disponíveis na seguinte ligação: https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

(198) 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. Diferente da interceção, a aquisição e a conservação de dados de comunicações não se destinam a obter o conteúdo da comunicação, mas sim a obter informações tais como o assinante de um serviço telefónico ou uma fatura discriminada. Pode incluir-se aqui o momento e a duração da comunicação, o número ou o endereço de correio eletrónico da entidade de origem e do destinatário e, por vezes, a localização dos dispositivos a partir dos quais a telecomunicação foi efetuada ([313]).

(199) Importa referir que a conservação e a aquisição de dados de comunicações não dirão normalmente respeito aos dados pessoais dos titulares de dados da UE transferidos ao abrigo da presente decisão para o Reino Unido. A obrigação de conservar ou divulgar dados de comunicações nos termos das partes 3 e 4 do IPA 2016 abrange os dados recolhidos pelos operadores de telecomunicações no Reino Unido diretamente junto dos utilizadores de um serviço de telecomunicações ([314]). Este tipo de tratamento «voltado para o cliente» não envolve normalmente uma transferência com base na presente decisão, ou seja, uma transferência de um responsável pelo tratamento/ /subcontratante na UE para um responsável pelo tratamento/subcontratante no Reino Unido.

(200) No entanto, por uma questão de exaustividade, as condições e as garantias que regem estes regimes de aquisição e de conservação são analisadas nos considerandos seguintes.

(201) Como premissa, importa notar que a conservação e a aquisição direcionadas de dados de comunicações estão disponíveis tanto para as agências de segurança nacional como para determinadas autoridades de aplicação da lei ([315]). As condições para exigir a conservação e/ou a aquisição de dados de comunicações podem variar consoante o motivo para solicitar a medida, ou seja, uma finalidade de segurança nacional ou de aplicação da lei.

(202) Em especial, embora o novo regime tenha introduzido o requisito geral de uma autorização *ex ante* por um organismo independente que será aplicável em todos os casos em que os dados de comunicação são conservados e/ou adquiridos (para uma finalidade de aplicação da lei ou de segurança nacional), na sequência do acórdão Tele2/Watson do Tribunal de Justiça da União Europeia ([316]), foram introduzidas garantias específicas quando a medida é solicitada para efeitos de aplicação da lei. Em especial, quando a conservação ou a aquisição de dados de comunicação é solicitada para uma finalidade de aplicação da lei, a autorização *ex ante* deve ser sempre concedida pelo comissário para os poderes de investigação. Nem sempre é esse o caso quando a medida é solicitada para uma finalidade de segurança nacional, uma vez que, tal como descrito abaixo, em determinados casos esse tipo de medidas pode ser autorizado por diferentes «titulares da autorização». Além disso, o novo regime elevou para «criminalidade grave» o limiar para o qual a conservação e a aquisição de dados de comunicações podem ser autorizadas ([317]).

([313]) Os dados de comunicações são definidos na *Section 261(5)* do IPA 2016. Os dados de comunicações dividem-se em «dados de eventos» [quaisquer dados que identifiquem ou descrevam um evento, por referência ou não à sua localização, num sistema de telecomunicações ou através de um sistema de telecomunicações em que o evento consista em uma ou mais entidades a efetuar uma atividade específica num determinado momento) e «dados da entidade» (quaisquer dados que a) se refiram a i) uma entidade, ii) uma associação entre um serviço de telecomunicações e uma entidade, ou iii) uma associação entre qualquer parte de um sistema de telecomunicações e uma entidade, b) consistam em ou incluam dados que identifiquem ou descrevam a entidade (por referência ou não à localização da entidade) e c) não sejam dados de eventos].

([314]) Isto resulta da definição de dados de comunicações prevista na *section 261(5)* do IPA 2016, segundo a qual os dados de comunicações são detidos ou obtidos por um operador de telecomunicações e dizem respeito ao utilizador de um serviço de telecomunicações e estão relacionados com a prestação desse serviço ou estão incluídos, fazem parte, estão ligados ou logicamente associados a uma comunicação [ver também o *Code of Practice on Communications Data* (código de boas práticas sobre dados de comunicações), disponível na seguinte ligação https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/ /757850/Communications_Data_Code_of_Practice.pdf, pontos 2.22 a 2.33]. Além disso, a definição de operador de telecomunicações prevista na *section 261(10)* do IPA 2016 exige que um operador de telecomunicações seja uma pessoa que disponibilize ou preste um serviço de telecomunicações a pessoas no Reino Unido ou que controle ou forneça um sistema de telecomunicações que se encontra (total ou parcialmente) no Reino Unido ou é controlado a partir do Reino Unido. Estas definições tornam claro que as obrigações ao abrigo do IPA 2016 não podem ser impostas aos operadores de telecomunicações cujo equipamento não se encontre no Reino Unido ou não seja controlado a partir do Reino Unido e que não ofereçam nem prestem serviços a pessoas no Reino Unido [ver também o *Code of Practice on Communications Data* (código de boas práticas sobre dados de comunicações), ponto 2.1]. Se os assinantes da UE (quer estejam localizados na UE ou no Reino Unido) utilizassem serviços no Reino Unido, quaisquer comunicações relacionadas com a prestação destes serviços seriam recolhidas diretamente pelo prestador de serviços no Reino Unido e não sujeitas a uma transferência da UE.

([315]) As autoridades competentes encontram-se elencadas no *schedule 4* do IPA 2016 e incluem as forças policiais, os serviços de informações, alguns ministérios e departamentos do Estado, a *National Crime Agency*, o *Her Majesty's Revenue and Customs*, a *Competition and Markets Authority*, o comissário para a informação, serviços de ambulância, bombeiros e de salvamento e as autoridades, por exemplo, no domínio da saúde e da segurança alimentar.

([316]) Processos apensos C-203/15 e C-698/15, Tele2/Watson, ECLI:EU:C:2016:970).

([317]) Ver *section 61.7(b)* no que se refere à aquisição de dados de comunicações e *section 87.10A* no que se refere à conservação de dados de comunicações.

i) *Autorização para a obtenção de dados de comunicações*

(203) De acordo com a parte 3 do IPA 2016, as autoridades públicas competentes estão autorizadas a obter dados de comunicações de um operador de telecomunicações ou de qualquer pessoa capaz de obter e divulgar esses dados. A autorização não pode permitir a interceção do conteúdo das comunicações ([318]) e deixa de produzir efeitos decorrido um mês ([319]), com a possibilidade de ser renovada mediante uma autorização adicional ([320]). A aquisição de dados de comunicações requer uma autorização do comissário para os poderes de investigação (IPC) ([321]) (a respeito do estatuto e dos poderes do IPC, ver os considerandos 250 a 251). Tal é sempre o caso quando a aquisição de dados de comunicações é solicitada por uma autoridade de aplicação da lei competente. No entanto, de acordo com a *section 61* do IPA 2016, quando os dados forem obtidos por razões de segurança nacional ou de bem-estar económico do Reino Unido, desde que os mesmos sejam relevantes para a segurança nacional ou quando um pedido for apresentado por um membro de um serviço de informações ao abrigo da *section 61(7)(b)* ([322]), a aquisição pode ser autorizada em alternativa ([323]) pelo comissário para os poderes de investigação ou por um dirigente superior designado ([324]). O dirigente designado deve ser independente da investigação ou da operação em causa e ter conhecimentos práticos sobre os princípios e a legislação em matéria de direitos humanos, nomeadamente os relativos à necessidade e à proporcionalidade ([325]). A decisão tomada pelo dirigente designado estará sujeita à supervisão *ex post* realizada pelo comissário para os Poderes de Supervisão (ver o considerando 254 para mais pormenores sobre as funções de supervisão *ex post* do comissário para os Poderes de Supervisão).

(204) A autorização para obter dados de comunicação baseia-se numa avaliação da necessidade e da proporcionalidade da medida. Mais especificamente, a necessidade da medida é apreciada à luz dos motivos enumerados na legislação ([326]). Tendo em conta a natureza específica desta medida, deve também ser necessária para uma investigação ou operação específica ([327]). O *Code of Practice on Communication Data* (código de boas práticas sobre dados de comunicações) estabelece outros requisitos em matéria de avaliação da necessidade das medidas ([328]). Nomeadamente, este código prevê que o pedido apresentado pela autoridade requerente deve identificar três elementos mínimos para justificar a necessidade desse pedido: i) o evento sob investigação, como, por exemplo, uma infração penal ou a localização de uma pessoa vulnerável desaparecida, ii) a pessoa cujos dados são solicitados, tais como suspeitos, testemunhas ou pessoas desaparecidas, e a forma como está ligada ao evento e iii) os dados de comunicações solicitados, tais como um número de telefone ou endereço IP, e a forma como esses dados estão relacionados com a pessoa e o evento ([329]).

(205) Além disso, a aquisição de dados de comunicações tem de ser proporcional ao que se pretende alcançar ([330]). O *Code of Practice on Communication Data* (código de boas práticas sobre dados de comunicações) esclarece que, ao proceder a essa avaliação, o titular da autorização deve proceder a um exercício de ponderação entre «a extensão da interferência nos direitos e liberdades de uma pessoa e um benefício específico para a investigação ou operação realizada por uma autoridade pública competente no interesse público e que, tendo em conta todas as considerações de um caso

([318]) *Section 60A(6)* do IPA 2016.

([319]) Este prazo é reduzido para três dias quando a autorização for concedida por razões de urgência [*section 65(3)* do IPA 2016].

([320]) Nos termos da *section 65* do IPA 2016, a renovação da autorização terá uma duração de um mês a contar da data de caducidade da autorização atual. A pessoa que concedeu a autorização pode cancelá-la em qualquer momento se considerar que os requisitos deixaram de se mostrar satisfeitos.

([321]) *Section 60A(1)* do IPA 2016. O gabinete para as autorizações de dados de comunicações (OCDA) desempenha esta função em nome do IPC (ver o código de boas práticas sobre dados de comunicações, n.º 5.6).

([322]) O pedido ao abrigo da *section 61(7)(b)*, do IPA 2016 é apresentado para fins criminosos aplicáveis, ou seja, em conformidade com a *section 61(7)*A, do IPA 2016: «se os dados de comunicações forem dados, no todo ou em parte, relativos a eventos, a finalidade de prevenir ou detetar a criminalidade grave; em qualquer outro caso, a finalidade de prevenção ou deteção da criminalidade ou de defensa da ordem».

([323]) O *Code of Practice on Communications Data* especifica que «quando um pedido relativo à segurança nacional possa ser apresentado ao abrigo da *section 60A* ou da *section 61*, a decisão sobre a via de autorização mais adequada num determinado caso é da competência das autoridades públicas. As autoridades públicas que pretendam recorrer à via do dirigente superior designado devem dispor de orientações claras sobre o momento em que esta via de autorização é adequada» [*Code of Practice on Communications Data* (código de boas práticas relativas a dados de comunicações), ponto 5. 19, disponível na seguinte ligação: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/822817/Communications_Data_Code_of_Practice.pdf].

([324]) A *section 70(3)* do IPA 2016 estabelece a definição de «dirigente designado», que varia em função da entidade pública pertinente (tal como previsto no *schedule* 4 do IPA 2016).

([325]) O código de boas práticas sobre dados de comunicações apresenta mais informações sobre a independência do dirigente superior designado (*Communications Data Code of Practice*, n.os 4.12 a 4.17, ver a nota de rodapé 323).

([326]) Os fundamentos são: i) a segurança nacional, ii) a prevenção ou deteção da criminalidade ou a defesa da ordem (no caso de «dados de eventos», apenas criminalidade grave), iii) no interesse do bem-estar económico do Reino Unido, na medida em que esse interesse seja igualmente relevante para o interesse da segurança nacional, iv) no interesse da segurança pública, v) para efeitos de prevenção da morte, lesões ou danos para a saúde física ou mental de uma pessoa, ou de atenuação de lesões ou danos para a saúde física ou mental de uma pessoa, vi) prestar assistência na investigação de alegados erros judiciários ou vii) identificar uma pessoa falecida ou incapaz de se identificar a si mesma devido a uma determinada condição [*section 61(7)* do IPA 2016].

([327]) *Section 60A(1)(b)* do IPA 2016.

([328]) *Code of Practice on Communications Data*, pontos 3.3 e seguintes, ver a nota de rodapé 323.

([329]) *Code of Practice on Communications Data*, ponto 3.13, ver a nota de rodapé 323.

([330]) *Section 60(1)(c)* do IPA 2016.

específico, uma interferência nos direitos de um indivíduo pode também não se justificar porque o impacto negativo nos direitos de outra pessoa ou grupo de pessoas é demasiado grave». Além disso, a fim de avaliar especificamente a proporcionalidade da medida, o código enumera uma série de elementos que devem ser incluídos no pedido apresentado pela autoridade requerente ([331]). Além disso, deve ser dada especial atenção ao tipo de dados de comunicações (dados de «entidade» ou «eventos» ([332])) a obter e privilegiar-se a utilização de categorias de dados menos intrusivas ([333]). O *Code of Practice on Communication Data* (código de boas práticas sobre dados de comunicações) contém igualmente instruções específicas para autorizações que envolvam dados de comunicações de pessoas em determinadas profissões (tais como médicos, advogados, jornalistas, deputados ou ministros do culto) ([334]) que são objeto de salvaguardas adicionais ([335]).

ii) *Notificação a exigir a conservação de dados de comunicações*

(206) A parte 4 do IPA 2016 estabelece as regras relativas à conservação de dados de comunicações e, em especial, os critérios que permitem ao ministro da tutela emitir uma notificação de conservação ([336]). As garantias introduzidas pelo IPA são as mesmas quando os dados são conservados para efeitos de aplicação da lei ou no interesse da segurança nacional.

(207) A emissão de tais notificações de conservação 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 ([337]). 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 do IPA 2016 e descrita nos considerandos 203 a 205.

(208) O exercício do poder para solicitar a conservação de determinados dados está sujeito a um conjunto de limitações e de garantias. O ministro da tutela só pode emitir uma notificação de conservação para um ou vários operadores ([338]) se considerar que a obrigação de conservar os dados é necessária para uma das finalidades legais ([339]) e é proporcional ao que se pretende alcançar ([340]). Conforme clarificado pelo próprio IPA

([331]) As informações a incluir devem conter: i) uma descrição geral da forma como a obtenção dos dados beneficiará a investigação ou a operação, ii) uma explicação da relevância dos intervalos de tempo solicitados, incluindo a forma como os mesmos são proporcionais ao evento objeto da investigação, iii) uma explicação do modo como se justifica o nível de intrusão quando se tem em conta o benefício que os dados proporcionarão à investigação (esta justificação deve incluir a ponderação da possibilidade de se realizar investigações menos intrusivas para alcançar o objetivo), iv) uma análise dos direitos (nomeadamente o direito à privacidade e, nos casos pertinentes, de liberdade de expressão) da pessoa em causa e um equilíbrio entre estes direitos e o benefício para a investigação, v) pormenores sobre que intrusão colateral pode ocorrer e a forma como os intervalos de tempo solicitados têm impacto na intrusão colateral [*Code of Practice on Communication Data* (código de boas práticas sobre dados de comunicações), pontos 3.22 a 3.26, ver a nota de rodapé 323].

([332]) Ver a nota de rodapé 313.

([333]) Quando se procuram obter dados de comunicações mais intrusivos (ou seja, dados de eventos), o código especifica que é mais adequado adquirir dados de primeira entidade ou adquirir diretamente dados relativos a eventos em casos limitados de urgência específica [*Code of Practice on Communication Data* (código de boas práticas sobre dados de comunicações), pontos 6.10 a 6.14, ver a nota de rodapé 323].

([334]) *Code of Practice on Communication Data* (código de boas práticas sobre dados de comunicações), pontos 8.8 a 8.44, ver a nota de rodapé 323.

([335]) O código de boas práticas especifica que «o titular da autorização deve ter especial cuidado ao analisar esses pedidos, incluindo uma análise adicional sobre se os pedidos podem ter consequências indesejadas e se o interesse público é mais bem servido pelo pedido» [*Code of Practice on Communication Data* (código de boas práticas sobre dados de comunicações), ponto 8.8]. Além disso, devem ser conservados registos para este tipo de pedidos e, aquando da próxima inspeção, esses pedidos devem ser assinalados à atenção do comissário para os poderes de investigação [*Code of Practice on Communication Data* (código de boas práticas sobre dados de comunicações), ponto 8.10, ver a nota de rodapé 323].

([336]) *Sections 87* a *89* do IPA 2016.

([337]) Nos termos da *section 90* do IPA 2016, um operador de telecomunicações ao qual seja enviado uma notificação de conservação pode solicitar uma análise ao ministro da tutela que o emitiu.

([338]) Nos termos da *section 87(2)(a)* do IPA 2016, uma notificação de conservação pode dizer respeito «a um determinado operador ou a qualquer descrição dos operadores».

([339]) As finalidades são i) o interesse da segurança nacional, ii) a finalidade da infração penal aplicável (tal como definido na *section 87.10A* do IPA 2016), iii) o interesse do bem-estar económico do Reino Unido, na medida em que esse interesse seja igualmente relevante para o interesse da segurança nacional, iv) o interesse da segurança pública, v) para efeitos de prevenção da morte, lesões ou danos para a saúde física ou mental de uma pessoa, ou de atenuação de lesões ou danos para a saúde física ou mental de uma pessoa, ou vi) apoiar investigações sobre alegados erros judiciários (*section 87* do IPA).

([340]) Ver a *section 87* do IPA 2016. Além disso, de acordo com o código de boas práticas pertinente, a fim de avaliar a proporcionalidade da notificação de conservação, aplicam-se os critérios previstos na *section 2(2)* do IPA 2016, nomeadamente o requisito de avaliar se o que se pretende alcançar com a notificação pode, na medida do razoável, ser alcançado com recurso a meios menos intrusivos. À semelhança da avaliação da proporcionalidade relativa à aquisição de dados de comunicações, o *Code of Practice on Communication Data* (código de boas práticas sobre dados de comunicações) esclarece que tal avaliação implica uma ponderação entre o alcance da interferência no direito à privacidade de uma pessoa e um benefício específico para a investigação [*Code of Practice on Communication Data* (código de boas práticas sobre dados de comunicações), ponto 16.3, ver a nota de rodapé 323].

2016 ([341]), antes de emitir uma notificação de conservação, o ministro da tutela deve ter em conta: os benefícios prováveis da notificação ([342]), uma descrição dos serviços de telecomunicações, a conveniência de limitar os dados a conservar por referência à localização ou a descrições das pessoas a quem são prestados serviços de telecomunicações ([343]), o número provável de utilizadores (quando conhecido) de qualquer serviço de telecomunicações a que se refere a notificação ([344]), a viabilidade técnica do cumprimento da notificação, os custos prováveis do cumprimento da notificação e quaisquer outros efeitos do mesmo para o operador de telecomunicações (ou descrição dos operadores) a que a notificação diz respeito ([345]). Tal como especificado no capítulo 17 do *Code of Practice on Communication Data* (código de boas práticas sobre dados de comunicações), todas as notificações de conservação têm de especificar cada tipo de dados a ser conservado e o modo como esse tipo de dados cumpre os testes necessários para a conservação.

(209) Em todos os casos (tanto para efeitos de segurança nacional como de aplicação da lei), a decisão do ministro da tutela de emitir a notificação de conservação deve ser aprovada por um comissário judicial independente no âmbito do chamado «procedimento de dupla segurança», que deve verificar, em especial, se a notificação para conservar os dados das comunicações relevantes é necessária e proporcionada para uma ou mais das finalidades legais ([346]).

3.3.1.1.3 Interferência em equipamentos

(210) A interferência em equipamentos é um conjunto de técnicas utilizadas para obter uma diversidade de dados a partir de equipamentos ([347]), que incluem computadores, *tablets* e telefones inteligentes, bem como cabos, fios e dispositivos de armazenamento ([348]). A interferência em equipamentos permite obter tanto o conteúdo das comunicações como os dados do equipamento ([349]).

(211) Em conformidade com a *section 13(1)* do IPA 2016, a utilização de interferências com equipamentos por parte de um serviço de informações implica uma autorização através de um mandado ao abrigo do procedimento de «dupla segurança» previsto pelo IPA 2016, desde que exista uma «ligação com as ilhas Britânicas» ([350]). De acordo com as explicações fornecidas pelas autoridades do Reino Unido, nas situações em que os dados sejam transferidos da

([341]) Ver a *section 88* do IPA 2016.

([342]) Os benefícios podem ser existentes ou previstos e devem respeitar as finalidades legais para as quais é possível conservar os dados [*Code of Practice on Communications Data*, ponto 17.17, ver a nota de rodapé 323].

([343]) Estas considerações incluirão determinar se o alcance geográfico total da notificação de conservação é necessário e proporcionado, bem como se é necessário e proporcionado incluir ou excluir determinadas descrições de pessoas [*Code of Practice on Communications Data*, ponto 17.17, ver a nota de rodapé 323].

([344]) Este procedimento ajudará o ministro da tutela a ponderar tanto o nível de intrusão nos clientes como os benefícios prováveis dos dados a conservar [*Code of Practice on Communications Data*, ponto 17.17, ver a nota de rodapé 323].

([345]) *Section 88* do IPA 2016.

([346]) *Section 89* do IPA 2016.

([347]) Nos termos das *sections 135(1)* e *198(1)* do IPA 2016, o termo «equipamentos» abrange os equipamentos que produzem emissões eletromagnéticas, acústicas ou de outro tipo e qualquer dispositivo suscetível de ser utilizado ligado a esses equipamentos.

([348]) *Code of Practice on Equipment Interference*, disponível na seguinte ligação: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715479/Equipment_Interference_Code_of_Practice.pdf, ponto 2.2.

([349]) Os dados relativos a equipamentos encontram-se definidos na *section 100* do IPA 2016 como dados de sistema e dados que a) estão incluídos, fazem parte, estão ligados ou logicamente associados a uma comunicação (pelo remetente ou por outro modo) ou a qualquer outro elemento de informação, b) podem ser logicamente separados do resto da comunicação ou do elemento de informação e c) caso assim sejam separados, não revelassem nada que, na medida do razoável, pudesse ser considerado como sendo o sentido (se for caso disso) da comunicação ou do elemento de informação.

([350]) Para que o requisito do mandado seja obrigatório, a *section 13(1)* do IPA 2016 exige igualmente que a conduta do serviço de informações constitua uma ou mais infrações nos termos das *sections 1* a *3A* do *Computer Misuse Act 1990* (Lei de 1990 relativa à Utilização Indevida de Computadores), o que seria o caso na grande maioria das circunstâncias, ver o *Code of Practice on Equipment Interference*, pontos 3.32 e 3.6 a 3.9. Nos termos da *section 13(2)* do IPA 2016, existe uma «ligação com as ilhas Britânicas» se a) qualquer conduta ocorrer nas ilhas Britânicas (independentemente da localização do equipamento que seria ou possa vir a ser objeto de interferência), b) o serviço de informações considerar que qualquer equipamento que esteja ou possa vir a ser objeto de interferência esteja, ou possa vir a estar no território das ilhas Britânicas, durante o decurso da interferência, ou c) interferência tiver por finalidade obter i) comunicações enviadas por uma pessoa ou a uma pessoa que esteja ou que o serviço de informações considere estar naquele momento nas ilhas Britânicas, ii) informações privadas relacionadas com uma pessoa que esteja ou que o serviço de informações considere estar nas ilhas Britânicas, ou iii) dados de equipamentos que sejam parte ou estejam ligados a comunicações ou informações privadas abrangidas pelas subalíneas i) e ii).

União Europeia para o Reino Unido no âmbito da presente decisão, existiria sempre uma «ligação com as ilhas Britânicas» e qualquer interferência em equipamentos que abrangesse esses dados estaria, por conseguinte, sujeita ao requisito do mandado obrigatório previsto na *section 13(1)* do IPA 2016 ([351]).

(212) As regras relativas aos mandados direcionados de interferência em equipamentos encontram-se estabelecidas na parte 5 do IPA 2016. À semelhança da interceção direcionada, a interferência direcionada em equipamentos tem de estar relacionada com um «alvo» específico, que tem de ser descrito no mandado ([352]). Os pormenores sobre a forma como um «alvo» deve ser identificado dependem do assunto e do tipo de equipamento a ser objeto de interferência. Em especial, a *section 115(3)* do IPA especifica os elementos que devem ser incluídos no mandado (por exemplo, nome da pessoa ou organização, descrição da localização), dependendo, por exemplo, de a interferência respeitar a um equipamento que pertence, é utilizado ou está na posse de uma determinada pessoa, organização ou grupo de pessoas, se encontra num local específico, etc. ([353]) As finalidades para as quais podem ser emitidos mandados direcionados de interferência em equipamentos dependem da autoridade pública que faz o pedido ([354]).

(213) À semelhança da interceção direcionada, a autoridade emissora deve ponderar se a medida é necessária para alcançar um objetivo específico e se é proporcional ao que se pretende alcançar ([355]). Além disso, deve igualmente ponderar se existem salvaguardas em matéria de segurança, conservação e divulgação, bem como em relação à «divulgação no estrangeiro» ([356]) (ver o considerando 196).

(214) O mandado tem de ser aprovado por um comissário judicial, exceto em casos urgentes ([357]). Neste último caso, o comissário judicial tem de ser informado de que foi emitido um mandado e deve aprová-lo no prazo de três dias úteis. No caso de o comissário judicial se recusar a aprová-lo, o mandado deixa de ter efeitos e não pode ser renovado ([358]). Além disso, o comissário judicial tem poderes para exigir o apagamento dos dados obtidos ao abrigo do mandado ([359]). O facto de um mandado ter sido emitido com caráter de urgência não afeta a supervisão *ex post* (ver os considerandos 244 a 255) nem as possibilidades de as pessoas singulares procurarem obter reparação (ver os considerandos 260 a 270). As pessoas singulares podem apresentar reclamação ao ICO ou apresentar uma reclamação contra qualquer alegado comportamento ao *Investigatory Powers Tribunal* da forma habitual. Em qualquer caso, o critério aplicado pelo comissário judicial ao decidir da aprovação de um mandado é o critério da necessidade e da proporcionalidade aplicável aos pedidos de interceção direcionada ([360]) (ver o considerando 192).

([351]) Por razões de exaustividade, importa referir que, mesmo em situações em que não existe uma «ligação com as ilhas Britânicas» e o recurso a interferências com equipamentos não está, por conseguinte, sujeita à exigência de um mandado obrigatório previsto na *section 13(1)* do IPA 2016, um serviço de informações que tencione desenvolver uma atividade para a qual possa obter um mandado de interferência em equipamentos em larga escala deve obter esse mandado por uma questão de princípio [ver *Code of Practice on Equipment Interference*, ponto 3.24]. Mesmo quando um mandado de interferência em equipamentos ao abrigo do IPA 2016 não seja juridicamente exigido nem obtido por uma questão de princípio, as medidas dos serviços de informações estão sujeitas a um conjunto de condições e limitações nos termos da *section 7* do *Intelligence Services Act 1994* (Lei de 1994 relativa aos Serviços de Informações). Inclui-se aqui, nomeadamente, a exigência de uma autorização do ministro da tutela, que deve certificar-se, em termos satisfatórios, de que qualquer medida não excede o necessário para o exercício adequado das funções do serviço de informações.

([352]) A *section 115* do IPA 2016 regula o conteúdo do mandado, especificando que deve incluir o nome ou a descrição das pessoas, organizações, localização ou grupo de pessoas que constituem o «alvo», uma descrição da natureza da investigação e uma descrição das atividades para as quais o equipamento é utilizado. Deve igualmente descrever o tipo de equipamento e a conduta que o destinatário do mandado está autorizado a ter.

([353]) Ver também o *Code of Practice on Equipment Interference*, ponto 5.7, ver a nota de rodapé 348.

([354]) As agências de segurança nacional podem apresentar um pedido para um mandado de interferência em equipamentos quando tal se mostre necessário para fins de segurança nacional, para efeitos de deteção da criminalidade grave e/ou no interesse do bem-estar económico do Reino Unido, na medida em que esse interesse seja igualmente relevante para o interesse da segurança nacional (*sections 102-103* do IPA 2016). Consoante a agência, pode ser solicitado um mandado de interferência em equipamentos para fins de aplicação da lei quando tal se mostre necessário para detetar ou prevenir um crime grave ou para prevenir a morte ou quaisquer lesões ou danos para a saúde física ou mental de uma pessoa, ou para atenuar quaisquer lesões ou danos para a saúde física ou mental de uma pessoa [ver a *section 106(1)* e *106(3)* do IPA 2016].

([355]) *Section 102(1)* do IPA 2016.

([356]) *Sections 129* a *131* do IPA 2016.

([357]) *Section 109* do IPA 2016.

([358]) *Section 109(4)* do IPA 2016.

([359]) *Section 110(3)* do IPA 2016. Nos termos do n.º 5.67 do *Code of Practice on Equipment Interference*, a urgência é determinada pela questão de saber se é razoavelmente praticável obter a aprovação do comissário judicial para a emissão do mandado no prazo disponível a fim de dar resposta a uma necessidade operacional ou de investigação. Os mandados urgentes devem enquadrar-se numa das seguintes categorias, ou em ambas: i) ameaça iminente à vida ou lesão grave — por exemplo, se uma pessoa for raptada e se se considerar que a sua vida está em perigo iminente; ou ii) uma oportunidade de recolha de informações ou de investigação com tempo limitado para agir — por exemplo, uma remessa de drogas de classe A está prestes a entrar no Reino Unido e os serviços de aplicação da lei pretendem abranger os autores de crimes graves a fim de proceder a detenções. Ver a nota de rodapé 348.

([360]) *Section 108* do IPA 2016.

(215) Por último, as salvaguardas específicas aplicáveis à interceção direcionada aplicam-se igualmente à interferência em equipamentos no que diz respeito à duração, renovação e alteração do mandado, bem como à interceção de deputados ao parlamento, de elementos sujeitos à prerrogativa legal de confidencialidade e de material jornalístico (ver mais pormenores no considerando 193).

3.3.1.1.4 Exercício de poderes em larga escala

(216) Os poderes em larga escala encontram-se regulados na parte 6 do IPA 2016. Além disso, os códigos de boas práticas preveem mais pormenores sobre o recurso aos poderes em larga escala. Embora não exista na legislação do Reino Unido uma definição de «poder em larga escala», no contexto do IPA 2016, foi descrita como sendo a recolha e conservação de grandes quantidades de dados obtidos pelo Estado com recurso a vários meios (ou seja, os poderes de interceção em larga escala, a aquisição em larga escala, a interferência em equipamentos em larga escala e os conjuntos de dados pessoais em larga escala) e que podem posteriormente ser acedidos pelas autoridades. Esta descrição é clarificada ao contrapor-se com o que o «poder em larga escala» não é: não equivale à chamada «vigilância em larga escala» sem limitações ou salvaguardas. Pelo contrário, como se explica de seguida, integra limitações e salvaguardas destinadas a garantir que o acesso aos dados não é facultado de forma indiscriminada ou injustificada ([361]). Em especial, os poderes em larga escala só podem ser utilizados se for estabelecida uma ligação entre a medida técnica que um serviço de informações nacional tenciona utilizar e o objetivo operacional para o qual essa medida é solicitada.

(217) Além disso, os poderes em larga escala estão disponíveis exclusivamente para os serviços de informações e são sempre objeto de um mandado emitido pelo ministro da tutela e aprovado por um comissário judicial. Ao escolher os meios de recolha de informações, há que ter em conta se o objetivo em questão pode ser prosseguido com recurso a «meios menos intrusivos» ([362]). Esta abordagem decorre do quadro legislativo que assenta no princípio da proporcionalidade e, por conseguinte, dá prioridade à recolha em larga escala.

3.3.1.1.4.1 Interceção em larga escala e interferência em equipamentos em larga escala

(218) O regime de interceção em larga escala está previsto na parte 6, capítulo 1, do IPA 2016, ao passo que o capítulo 3 da mesma parte regula a interferência em equipamentos em larga escala. Estes regimes são substancialmente idênticos, pelo que as condições e salvaguardas adicionais aplicáveis a estes mandados são analisadas em conjunto.

i) *Condições e critérios para a emissão do mandado*

(219) Um mandado de interceção em larga escala é limitado à interceção de comunicações no decurso da transmissão enviada ou recebida por pessoas que se encontram fora das ilhas Britânicas ([363]), as chamadas «comunicações relacionadas com o estrangeiro» ([364]), bem como outros dados pertinentes e a subsequente seleção para exame

([361]) De acordo com o relatório sobre os poderes em larga escala apresentado pelo Lorde David Anderson, revisor independente da legislação em matéria de terrorismo antes da aprovação do IPA 2016, «*deve ser claro que a recolha e a conservação de dados em larga escala não equivalem à chamada "vigilância em larga escala". Qualquer sistema jurídico digno desse nome incluirá limitações e salvaguardas destinadas precisamente a garantir que o acesso aos arquivos de dados sensíveis não é facultado de forma indiscriminada ou injustificada. Tais limitações e salvaguardas existem certamente no projeto de lei*». Lorde David Anderson, *Report of the bulk power review* (Relatório de análise ao poder em larga escala), agosto de 2016, ponto 1.9, disponível na seguinte ligação: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/546925/56730_Cm9326_WEB.PDF

([362]) *Section 2.2.* do IPA 2016. Ver, por exemplo, o *Code of Practice on Bulk Acquisition of Communications Data*, ponto 4.11, disponível na seguinte ligação: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715477/Bulk_Communications_Data_Code_of_Practice.pdf

([363]) As «ilhas Britânicas» constituem o Reino Unido, as ilhas Anglo-Normandas e a ilha de Man e estão definidas no *schedule 1* do *Interpretation Act 1978* (Lei de 1978 relativa à Interpretação de Leis), disponível na seguinte ligação: https://www.legislation.gov.uk/ukpga/1978/30/schedule/1

([364]) Nos termos da *section 136* do IPA 2016, entende-se por «comunicações relacionadas com o estrangeiro»: i) comunicações enviadas por pessoas que se encontram fora das ilhas Britânicas, ou ii) comunicações recebidas por pessoas que se encontram fora das ilhas Britânicas. Este regime, tal como confirmado pelas autoridades do Reino Unido, abrange igualmente as comunicações entre duas pessoas que se encontram ambas fora das ilhas Britânicas. A Grande Secção do Tribunal Europeu dos Direitos Humanos, no processo *Big Brother Watch e o./Reino Unido* (ver a nota de rodapé 279 acima), n.º 376, considerou, no que respeita a uma limitação semelhante (relativa às «comunicações externas») das comunicações que podem ser captadas por interceção em larga escala no âmbito do RIPA 2000, que era suficientemente delimitada e previsível.

do material intercetado ([365]). Um mandado de interferência em equipamentos em larga escala ([366]) autoriza o destinatário a proteger a interferência em qualquer equipamento com o objetivo de obter comunicações relacionadas com o estrangeiro (incluindo tudo o que inclua voz, música, sons, imagens visuais ou dados de qualquer natureza), dados dos equipamentos (dados que permitam ou facilitem o funcionamento de um serviço postal, um sistema de telecomunicações, um serviço de telecomunicações) ou qualquer outra informação ([367]).

(220) O ministro da tutela só pode emitir um mandado em larga escala a pedido do responsável de um serviço de informações ([368]). Um mandado que autorize uma interceção em larga escala ou uma interferência em equipamentos em larga escala só deve ser emitido se o mesmo for necessário para a segurança nacional e para outros fins de prevenção ou deteção da criminalidade grave, ou para o interesse do bem-estar económico do Reino Unido, quando relevante para a segurança nacional ([369]). Além disso, a *section 142(7)* do IPA 2016 exige que um mandado de interceção em larga escala seja objeto de uma maior especificação do que a simples referência ao «interesse da segurança nacional», ao «bem-estar económico do Reino Unido» e à «prevenção e combate à criminalidade grave», mas deve ser estabelecida uma ligação entre a medida que se procura obter e um ou mais objetivos operacionais que devem ser incluídos no mandado.

(221) A escolha da finalidade operacional resulta de um processo com vários níveis. A *section 142(4)* prevê que as finalidades operacionais especificadas no mandado devem ser especificadas numa lista mantida pelos responsáveis dos serviços de informações, como finalidades que consideram ser finalidades operacionais para as quais pode ser selecionado para exame conteúdo intercetado ou dados secundários obtidos ao abrigo de mandados de interceção em larga escala. A lista de finalidades operacionais deve ser aprovada pelo ministro da tutela. O ministro da tutela só pode dar essa aprovação se considerar que a finalidade operacional for especificada em maior detalhe do que os motivos gerais para autorizar o mandado (segurança nacional ou segurança nacional e bem-estar económico ou prevenção de criminalidade grave) ([370]). No final de cada período de três meses pertinente, o ministro da tutela deve fornecer uma cópia da lista de finalidades operacionais à *Intelligence and Security Committee* (comissão para a informação e a segurança) (ISC) do parlamento. Por último, o primeiro-ministro deve analisar a lista de finalidades operacionais pelo menos uma vez por ano ([371]). Conforme referido pelo *High Court*, «[n]ão devem ser consideradas salvaguardas insignificantes, uma vez que constituem, na sua globalidade, um conjunto complexo de modos de responsabilização, que envolvem o parlamento e os membros do governo ao mais alto nível» ([372]).

(222) Essas finalidades operacionais limitam igualmente o âmbito da seleção do material de interceção para a fase de exame. A seleção para exame de qualquer material recolhido ao abrigo do mandado em larga escala tem de se justificar tendo em conta a finalidade ou as finalidades operacionais. Tal como explicado pelas autoridades do Reino Unido, tal significa que os mecanismos práticos relativos ao exame devem ser avaliados pelo ministro da tutela já na fase do mandado, fornecendo informações suficientes para cumprir as obrigações legais previstas nas *sections 152* e *193* do IPA 2016 ([373]). Os pormenores fornecidos ao ministro da tutela relativamente a esses mecanismos teriam de incluir, por exemplo, informações (se for caso disso) sobre a forma como os mecanismos de filtragem podem variar durante o período em que um mandado produzirá efeitos ([374]). Para mais pormenores sobre o processo e as salvaguardas aplicadas às fases de filtragem e exame, ver o considerando 229.

([365]) *Section 136(4)* do IPA 2016. De acordo com as explicações recebidas do Governo do Reino Unido, a interceção em larga escala pode ser utilizada, por exemplo, para identificar ameaças anteriormente desconhecidas para a segurança nacional do Reino Unido, filtrando e analisando material intercetado a fim de identificar as comunicações com valor em termos de informações [(*Explanatory Framework section H: National security* (Secção H do quadro explicativo: segurança nacional), p. 27 e 28, ver a nota de rodapé 29]. Tal como explicado pelas autoridades do Reino Unido, esses instrumentos podem ser utilizados para estabelecer ligações entre suspeitos conhecidos, bem como para procurar indícios de atividade por pessoas que podem ainda não ser conhecidas, mas que surgem no decurso de uma investigação, e para identificar padrões de atividade que possam indicar uma ameaça para o Reino Unido.

([366]) Em conformidade com a *section 13(1)* do IPA 2016, o recurso a interferências com equipamentos por parte de um serviço de informações implica uma autorização através de um mandado ao abrigo do IPA 2016, desde que exista uma «ligação com as ilhas Britânicas», ver o considerando 211.

([367]) *Section 176* do IPA 2016. Um mandado de interferência em equipamentos em larga escala não pode autorizar uma conduta que (a menos que praticado com competência jurídica para o efeito) constitua uma interceção ilícita (exceto relativamente a uma comunicação armazenada). De acordo com o quadro explicativo do Reino Unido, as informações obtidas poderiam ser necessárias para identificar suspeitos e seriam normalmente operações de grande escala adequadas [*Explanatory Framework, section H: National security* (Secção H do quadro explicativo: segurança nacional), p. 28, ver a nota de rodapé 29].

([368]) *Section 138(1)* e *178(1)* do IPA 2016.

([369]) *Section 138(2)* e *178(2)* do IPA 2016.

([370]) De acordo com as explicações fornecidas pelas autoridades do Reino Unido, por exemplo, uma finalidade operacional pode limitar o âmbito da medida à existência de uma ameaça numa zona geográfica específica.

([371]) *Section 142(4)-(10)* do IPA 2016.

([372]) *High Court of Justice, Liberty*, [2019] EWHC 2057 (Admin.), n.º 167.

([373]) As *sections 152* e *193* do IPA 2016 exigem que: a) a seleção para exame seja efetuada apenas para as finalidades operacionais especificadas no mandado, b) a seleção para exame seja necessária e proporcionada em todas as circunstâncias e c) a seleção para exame não viole a proibição de selecionar material e identificar as comunicações que tenham sido enviadas ou destinadas a pessoas conhecidas das ilhas Britânicas nesse momento.

([374]) Ver o *Code of Practice on Interception of Communications*, ponto 6.6, ver a nota de rodapé 278.

(223) Um poder em larga escala só pode ser autorizado se for proporcional ao que se pretende alcançar ([375]). Tal como especificado no *Code of Practice on Interception*, qualquer avaliação da proporcionalidade implica ponderar a gravidade da intrusão na privacidade [e outras considerações enunciadas na *section 2(2)*] face à necessidade da atividade em termos de investigação, operacionais ou de capacidade. A conduta autorizada deve oferecer uma perspetiva realista de obtenção do benefício esperado, não devendo ser desproporcionada ou arbitrária ([376]). Como já foi referido, tal significa, na prática, que o teste da proporcionalidade assenta num teste de equilíbrio entre o que se pretende alcançar [«finalidade(s) operacional(ais)»] e as opções técnicas disponíveis (por exemplo, interceção direcionada ou em larga escala, interferência em equipamentos, aquisição de dados de comunicações), privilegiando o recurso a meios menos intrusivos (ver os considerandos 181 e 182). Quando mais do que uma medida se mostrar adequada ao objetivo, deve privilegiar-se o recurso a meios menos intrusivos.

(224) Uma garantia adicional sobre a avaliação da proporcionalidade da medida solicitada é assegurada pelo facto de o ministro da tutela dever receber as informações pertinentes necessárias para efetuar corretamente a sua avaliação. Em especial, o *Code of Practice on Interception* e o *Code of Practice on Equipment Interference* impõem que o pedido apresentado pela autoridade competente mencione o contexto do pedido, a descrição das comunicações a intercetar e os operadores de telecomunicações que devem prestar assistência, a descrição da conduta a autorizar, as finalidades operacionais e uma explicação das razões pelas quais a conduta é necessária e proporcionada ([377]).

(225) Por último e não menos importante, a decisão do ministro da tutela de emitir o mandado deve ser aprovada por um comissário judicial independente que aprecie a avaliação da necessidade e da proporcionalidade da medida proposta, recorrendo aos mesmos princípios que seriam utilizados por um tribunal num pedido de exame judiciário ([378]). Mais especificamente, o comissário judicial analisará as conclusões do ministro da tutela quanto a saber se o mandado é necessário e se a conduta é proporcionada à luz dos princípios estabelecidos na *section 2(2)* do IPA 2016 (deveres gerais em matéria de privacidade). O comissário judicial analisará igualmente as conclusões do ministro da tutela quanto à questão de saber se cada uma das finalidades operacionais especificadas no mandado constitui um objetivo para o qual a seleção é ou pode ser necessária. Se o comissário judicial se recusar a aprovar a decisão de emissão de um mandado, o ministro da tutela pode: i) acatar a decisão e, por conseguinte, não emitir o mandado, ou ii) reencaminhar o assunto para decisão do comissário para os poderes de investigação (a menos que este tenha sido quem tomou a decisão inicial) ([379]).

ii) *Salvaguardas adicionais*

(226) O IPA 2016 introduziu novos limites à duração, renovação e alteração de um mandado em larga escala. O mandado deve ter uma duração máxima de seis meses e qualquer decisão de renovação ou alteração (exceto alterações menores) deve ser igualmente aprovada por um comissário judicial ([380]). O *Code of Practice on Interception* e o *Code of Practice on Equipment Interference* especificaram que uma alteração das finalidades operacionais do mandado é considerada uma alteração importante do mandado ([381]).

([375]) *Sections 138(1)(b)* e *(c)* e *sections 178(b)* e *(c)* do IPA 2016.

([376]) *Code of Practice on Interception of Communications*, ponto 4.10, ver a nota de rodapé 278.

([377]) *Code of Practice on Interception of Communications*, ponto 6.20, ver a nota de rodapé 278, e *Code of Practice on Equipment Interference*, ponto 6.13, ver a nota de rodapé 348.

([378]) *Section 138(1)(g)* e *178(1)(f)* do IPA 2016. A autorização prévia de um organismo independente foi, nomeadamente, identificada pelo Tribunal Europeu dos Direitos Humanos como uma garantia importante contra os abusos no contexto da interceção em larga escala. Tribunal Europeu dos Direitos Humanos, *Big Brother Watch e o./Reino Unido* (ver a nota de rodapé 269 acima), n.os 351 e 352. Importa ter em conta que este acórdão dizia respeito ao anterior quadro jurídico (RIPA 2000), que não continha algumas das garantias (incluindo a autorização prévia de um comissário judicial independente) introduzidas pelo IPA 2016.

([379]) *Section 159(3)* e *(4)* do IPA 2016.

([380]) *Sections 143* a *146* e *184* a *188* do IPA 2016. Em caso de alteração urgente, o ministro da tutela pode proceder à alteração sem aprovação prévia, mas deve notificar o comissário e este deve então decidir se aprova ou recusa a alteração (*section 147* do IPA 2016). Os mandados devem ser anulados sempre que um mandado deixe de ser necessário ou proporcionado, ou que o exame do conteúdo intercetado, dos metadados ou de outros dados obtidos ao abrigo do mandado deixe de ser necessário para qualquer das finalidades operacionais especificadas no mandado (*sections 148* e *189* do IPA 2016).

([381]) *Code of Practice on Interception of Communications*, pontos 6.44 a 6.47, ver a nota de rodapé 278, e *Code of Practice on Equipment Interference*, ponto 6.48, ver a nota de rodapé 348.

(227) À semelhança do que está previsto para a interceção direcionada, a parte 6 do IPA 2016 prevê que o ministro da tutela deve assegurar a existência de disposições que preveem salvaguardas em matéria de conservação e divulgação do material obtido ao abrigo do mandado ([382]), bem como da divulgação no estrangeiro ([383]). Em especial, as *sections 150(5)* e *191(5)* do IPA 2016 exigem que todas as cópias de qualquer desses materiais recolhidos ao abrigo do mandado sejam armazenadas de forma segura e destruídas logo que deixem de existir motivos pertinentes para a sua conservação, enquanto as *sections 150(2)* e *191(2)* impõem a limitação ao mínimo necessário para as finalidades legais do número de pessoas a quem o material é divulgado e em que medida o material é divulgado, disponibilizado ou copiado ([384]).

(228) Por último, quando o material intercetado através de uma interceção em larga escala ou de uma interferência em equipamentos em larga escala deva ser entregue a um país terceiro («divulgações no estrangeiro»), o IPA 2016 prevê que o ministro da tutela deve assegurar a aplicação de mecanismos adequados para garantir a existência de salvaguardas semelhantes em matéria de segurança, conservação e divulgação nesse país terceiro ([385]). Além disso, a *section 109* do DPA 2018 estabelece requisitos específicos para transferências internacionais de dados pessoais pelos serviços de informações para países terceiros ou organizações internacionais e não permite que os dados pessoais sejam transferidos para um país ou território fora do Reino Unido ou para uma organização internacional, a menos que a transferência seja necessária e proporcionada para o exercício das funções legais do responsável pelo tratamento ou para outras finalidades previstos na *section 2(2)(a)* do *Security Service Act 1989* ou nas *sections 2(2)(a)* e *4(2)(a)* do *Intelligence Services Act 1994* ([386]). Importa notar que estes requisitos são igualmente aplicáveis nos casos em que é invocada a isenção relativa à segurança nacional nos termos da *section 110* do DPA 2018, uma vez que a *section 110* do DPA de 2018 não enumera a *section 109* do DPA 2018 como uma das disposições que não são suscetíveis de aplicação se for necessária uma isenção de determinadas disposições para efeitos de garantia da segurança nacional.

(229) Uma vez aprovado o mandado e os dados recolhidos em larga escala, os dados serão objeto de uma seleção antes de serem examinados. A fase de seleção e exame está sujeita a um novo teste de proporcionalidade realizado pelo analista que define os critérios de seleção, com base nas finalidades operacionais previstas no mandado (e nos eventuais mecanismos de filtragem). Tal como previsto nas *sections 152* e *193* do IPA, ao emitir o mandado, o ministro da tutela deve assegurar a existência de mecanismos para garantir que a seleção do material é efetuada apenas para as finalidades operacionais especificadas e que a mesma é necessária e proporcionada em todas as circunstâncias. A este respeito, as autoridades do Reino Unido esclareceram que o material intercetado em larga escala é selecionado, em primeiro lugar, através de filtragem automática com o objetivo de descartar dados que não sejam suscetíveis de ser de interesse para a segurança nacional. Os filtros variarão ocasionalmente (à medida que os padrões de tráfego na Internet, os tipos e os protocolos se alteram) e dependerão da tecnologia e do contexto operacional. Após esta fase, os dados só podem ser selecionados para exame se forem pertinentes para as finalidades operacionais especificadas no mandado ([387]). As garantias previstas pelo IPA 2016 para o exame do material recolhido aplicam-se a qualquer tipo de dados (tanto conteúdos intercetados como dados secundários) ([388]). As *sections 152* e *193* do IPA 2016 preveem igualmente uma proibição geral de selecionar material de exame respeitante a conversas enviadas por pessoas que se encontrem nas ilhas Britânicas ou destinadas a estas. Se as autoridades pretenderem examinar material deste tipo, devem apresentar um pedido de mandado de exame direcionado ao abrigo das partes 2 e 4 do IPA 2016, emitido pelo ministro da tutela e aprovado por um comissário judicial ([389]). Se uma pessoa selecionar deliberadamente conteúdo intercetado para exame em violação dos requisitos previstos na legislação ([390]), comete uma infração penal ([391]).

([382]) *Section 156* do IPA 2016.

([383]) *Sections 150* e *191* do IPA 2016.

([384]) A Grande Secção do Tribunal Europeu dos Direitos Humanos, no processo *Big Brother Watch e o./Reino Unido* (ver a nota de rodapé 268 acima), confirmou o sistema de garantias adicionais para a conservação, o acesso e a divulgação que foi previsto ao abrigo do RIPA 2000, ver n.os 392 a 394 e 402 a 405. O IPA 2016 prevê o mesmo sistema de garantias.

([385]) *Sections 151* e *192* do IPA 2016.

([386]) Para mais informações sobre estas finalidades, ver a nota de rodapé 312.

([387]) Os códigos relativos à interceção de comunicações especificam, a este respeito, que estes sistemas de tratamento tratam dados provenientes das ligações ou sinais de comunicações que a autoridade intercetora optou por intercetar. Em seguida, é aplicado um certo nível de filtragem ao tráfego nessas ligações e sinais, concebido para selecionar tipos de comunicações com potencial valor em termos de informações, ao mesmo tempo que se descartam as menos suscetíveis de terem valor em termos de informações. Em resultado desta filtragem, que variará entre os sistemas de tratamento, uma parte significativa das comunicações nessas ligações e sinais será automaticamente descartada. Poderão então efetuar-se outras pesquisas complexas para identificar outras comunicações mais suscetíveis de ter maior valor em termos de informações e relacionadas com as funções legais da agência. Estas comunicações podem então ser selecionadas para exame para uma ou mais das finalidades operacionais especificadas no mandado, se estiverem reunidas as condições de necessidade e proporcionalidade. Apenas os elementos que não tenham sido filtrados podem potencialmente ser selecionados para exame por pessoas autorizadas [*Code of Practice on Interception of Communications* (código de boas práticas sobre a interceção das comunicações), ponto 6.6, ver a nota de rodapé 278].

([388]) Ver *section 152(1)*, alíneas a) e b), do IPA 2016, segundo a qual o exame do tipo de dados (conteúdos intercetados e dados secundários) deve ser efetuado apenas para a finalidade especificada e ser necessário e proporcionado em todas as circunstâncias.

([389]) Este tipo de mandado não é exigido quando os dados relativos a pessoas que se encontram nas ilhas Britânicas são «dados secundários» (ver *section 152(1)*, alínea c), do IPA 2016).

([390]) *Sections 152* e *193* do IPA 2016.

([391]) *Sections 155* e *196* do IPA 2016.

(230) A avaliação da seleção do material efetuada pelo analista está sujeita a uma supervisão *ex post* pelo comissário para os poderes de investigação, que avalia a conformidade com as salvaguardas específicas estabelecidas no IPA 2016 para a fase de exame ([392]) (ver igualmente o considerando 229). O comissário para os poderes de investigação deve acompanhar (nomeadamente através de auditoria, inspeção e investigação) o exercício, pelas autoridades públicas, dos poderes de investigação mencionados no IPA 2016 ([393]). A este respeito, o *Code of Practice on Interception* e o *Code of Practice on Equipment Interference* esclarecem que a agência deve conservar registos para efeitos de exames e auditorias subsequentes, devendo esses registos indicar as razões pelas quais o acesso ao material por parte de pessoas autorizadas é necessário e proporcionado, bem como as finalidades operacionais aplicáveis ([394]). Por exemplo, no seu relatório anual de 2018, o *Investigatory Powers Commissioner Office* (IPCO, Gabinete do Comissário para os Poderes de Investigação) ([395]) concluiu que as justificações registadas pelos analistas para o exame de determinado material recolhido em larga escala cumpriam a norma exigida de proporcionalidade, fornecendo informações suficientes sobre as razões das suas «consultas» em relação à finalidade a alcançar ([396]). No seu relatório de 2019, o IPCO, no que se refere aos poderes em larga escala, declarou claramente a sua intenção de prosseguir as inspeções das interceções em larga escala, incluindo um exame pormenorizado dos seletores e dos critérios de pesquisa ([397]). Continuará igualmente a controlar cuidadosamente, numa base casuística, a escolha das medidas de vigilância (direcionadas contra em larga escala), tanto durante a sua ponderação sobre os pedidos de mandado no âmbito da dupla segurança, como durante as inspeções ([398]). Este acompanhamento complementar será devidamente tido em conta no contexto do acompanhamento da presente decisão pela Comissão, a que se referem os considerandos 281 a 284.

3.3.1.1.4.2 Aquisição em larga escala de dados de comunicações

(231) O capítulo 2 da parte 6 do IPA 2016 regula os mandados de aquisição em larga escala que autorizam o destinatário a exigir a um operador de telecomunicações que divulgue ou obtenha quaisquer dados de comunicações na posse do operador. Estes mandados autorizam igualmente a autoridade requerente a selecionar os dados para a fase seguinte do exame. Tal como no caso da conservação e aquisição direcionadas de dados de comunicações (ver o considerando 199), em regra a aquisição em larga escala de dados de comunicações também não diz respeito a dados pessoais de titulares de dados da UE transferidos ao abrigo da presente decisão para o Reino Unido. A obrigação de divulgar dados de comunicações nos termos da parte 6, capítulo 2, do IPA 2016 abrange os dados recolhidos pelos operadores de telecomunicações no Reino Unido diretamente junto dos utilizadores de um serviço de telecomunicações ([399]). Este tipo de tratamento «voltado para o cliente» não envolve normalmente uma transferência com base na presente decisão, ou seja, uma transferência de um responsável pelo tratamento/subcontratante na UE para um responsável pelo tratamento/ /subcontratante no Reino Unido.

(232) No entanto, por uma questão de exaustividade, descrevem-se de seguida as condições e as salvaguardas que regem a aquisição de dados de comunicações em larga escala.

([392]) *Sections 152* e *193* do IPA 2016.

([393]) *Section 229* do IPA 2016.

([394]) *Code of Practice on Interception of Communications*, ponto 6.74, ver a nota de rodapé 278, e *Code of Practice on Equipment Interference*, ponto 6.78, ver a nota de rodapé 348.

([395]) O IPCO foi constituído ao abrigo da *section 238* do IPA 2016 para fornecer ao comissário para os poderes de investigação o pessoal, o alojamento, o equipamento e outros serviços necessários para o desempenho das suas funções (ver o considerando 251).

([396]) O relatório anual de 2018 do IPCO especificou que as justificações registadas pelos analistas do GCHQ cumpriam a norma exigida e os analistas estavam a ter em conta a proporcionalidade das suas consultas de dados em larga escala em suficiente detalhe. Relatório anual de 2018 do comissário para os poderes de investigação, ponto 6.22, ver a nota de rodapé 464.

([397]) Relatório anual de 2019 do comissário para os poderes de investigação, ponto 7.6, ver a nota de rodapé 463.

([398]) Relatório anual de 2019 do comissário para os poderes de investigação, ponto 10.22, ver a nota de rodapé 463.

([399]) Isto decorre da definição de dados de comunicações prevista na *section 261(5)* do IPA 2016, segundo a qual os dados de comunicações são detidos ou obtidos por um operador de telecomunicações e dizem respeito ao utilizador de um serviço de telecomunicações e estão relacionados com a prestação desse serviço, ou estão incluídos, fazem parte, estão ligados ou logicamente associados a uma comunicação (ver também o *Code of Practice on Bulk Acquisition of Communications Data*), disponível na seguinte ligação: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715477/Bulk_Communications_Data_Code_of_Practice.pdf, pontos 2.15 a 2.22]. Além disso, a definição de operador de telecomunicações prevista na *section 261(10)* do IPA 2016 exige que um operador de telecomunicações seja uma pessoa que disponibilize ou preste um serviço de telecomunicações a pessoas no Reino Unido ou que controle ou forneça um sistema de telecomunicações que se encontra (total ou parcialmente) no Reino Unido ou é controlado a partir do Reino Unido. Estas definições tornam claro que as obrigações ao abrigo do IPA 2016 não podem ser impostas aos operadores de telecomunicações cujo equipamento não se encontre no Reino Unido ou não seja controlado a partir do Reino Unido e que não ofereçam nem prestem serviços a pessoas no Reino Unido (ver também o *Code of Practice on Bulk Acquisition of Communications Data*, ponto 2.2). Se os assinantes da UE (quer estejam localizados na UE, quer no Reino Unido) utilizassem serviços no Reino Unido, quaisquer comunicações relacionadas com a prestação destes serviços seriam recolhidas diretamente pelo prestador de serviços no Reino Unido e não sujeitas a uma transferência da UE.

(233) O IPA 2016 substitui a legislação relativa à aquisição de dados de comunicações em larga escala, que foi objeto do acórdão do TJUE no processo Privacy International. A legislação em causa nesse processo foi revogada e o novo regime prevê condições e garantias específicas ao abrigo das quais é possível autorizar uma medida deste tipo.

(234) Nomeadamente, ao contrário do que sucedia no regime anterior, ao abrigo do qual o ministro da tutela dispunha de plenos poderes discricionários para autorizar a medida ([400]), o IPA 2016 exige que o ministro da tutela emita um mandado apenas se a medida for necessária e proporcionada. Isto significa, na prática, que deve existir uma ligação entre o acesso aos dados e o objetivo prosseguido ([401]). Mais especificamente, o ministro da tutela terá de avaliar a existência de uma ligação entre a medida solicitada e uma ou mais «finalidades operacionais» indicadas no mandado (ver o considerando 219); no que diz respeito à avaliação da proporcionalidade, o código de boas práticas pertinente especifica que o ministro da tutela deve ter em conta se o que se pretende alcançar pelo mandado pode razoavelmente ser alcançado por outros meios menos intrusivos [*section 2(2)(a)* da lei]. Por exemplo, obter as informações necessárias através de um poder menos intrusivo, como, por exemplo, a aquisição direcionada de dados de comunicações ([402]).

(235) Para proceder a essa avaliação, o ministro da tutela basear-se-á em informações que os responsáveis pelos serviços de informações ([403]) são obrigados a apresentar no respetivo pedido, tais como as razões pelas quais a medida é considerada necessária por um dos motivos legais e as razões pelas quais o objetivo pretendido não pode ser razoavelmente alcançado por outros meios menos intrusivos ([404]). Além disso, as finalidades operacionais limitam o âmbito para o qual os dados obtidos ao abrigo do mandado podem ser selecionados para exame ([405]). Tal como especificado no código de boas práticas pertinente, as finalidades operacionais devem descrever um requisito claro e conter dados suficientemente pormenorizados para o ministro da tutela considerar, de forma satisfatória, que os dados adquiridos só podem ser selecionados para exame por razões específicas ([406]). Com efeito, o ministro da tutela, antes de autorizar o mandado, deverá assegurar-se da existência de mecanismos específicos para garantir que só são selecionados os elementos considerados necessários para exame para uma finalidade operacional e para uma finalidade legal, devendo ser proporcionados e necessários em todas as circunstâncias. Este requisito específico, consagrado nas *sections 158* e *172* ([407]) do IPA 2016, relativo à avaliação prévia da necessidade e proporcionalidade dos critérios utilizados para efeitos da seleção representa outra novidade importante do regime introduzido pelo IPA 2016 em comparação com o regime anteriormente em vigor.

(236) O IPA 2016 introduziu igualmente a obrigação de o ministro da tutela assegurar, antes de emitir o mandado para a aquisição em larga escala de dados de comunicações, que existem limitações específicas em matéria de segurança, conservação e divulgação dos dados pessoais recolhidos ([408]). Em caso de divulgação no estrangeiro, as salvaguardas, descritas no considerando 227, para a interceção em larga escala e a interferência em equipamentos em larga escala também se aplicam neste contexto ([409]). A legislação relativa à duração ([410]), renovação ([411]) e alteração dos mandados em larga escala ([412]) estabelece outros limites.

(237) É importante salientar que, tal como no caso dos outros poderes em larga escala, antes de emitir o mandado, o ministro da tutela necessita da aprovação de um comissário judicial ([413]). Esta é uma característica fundamental do regime instituído pelo IPA 2016.

([400]) A *section 94(1)* do *Telecommunication Act 1984* (Lei de 1984 relativa às Comunicações) dispunha que o ministro da tutela podia emitir instruções de caráter geral que lhe pareçam necessárias ou oportunas no interesse da segurança nacional (ver a nota de rodapé 451).

([401]) Ver o acórdão Privacy International, n.º 78.

([402]) Ver o *Code of Practice on Bulk Acquisition of Communications Data*, ponto 4.11 (ver a nota de rodapé 399414).

([403]) Um mandado de aquisição em larga escala só pode ser solicitado pelos responsáveis dos serviços de informações que sejam: i) o diretor-geral do serviço de segurança (*Director General of the Security Service*), ii) o diretor do serviço de informações secretas (*Chief of the Secret Intelligence Service*), ou iii) o diretor do GCHQ (ver *sections 158* e *263* do IPA 2016).

([404]) *Code of Practice on Bulk Acquisition of Communications Data*, ponto 4.5 (ver a nota de rodapé 399).

([405]) Nos termos da *section 161* do IPA 2016, os objetivos operacionais especificados no mandado devem ser os especificados numa lista mantida pelos responsáveis dos serviços de informações («lista de finalidades operacionais»), como objetivos que consideram serem fins operacionais para os quais os dados de comunicações obtidos com base em certificados de aquisição agrupados podem ser selecionados para exame.

([406]) *Code of Practice on Bulk Acquisition of Communications Data*, ponto 6.6 (ver a nota de rodapé 399).

([407]) A *section 172* do IPA 2016 exige que sejam estabelecidas salvaguardas específicas para a fase de filtragem e seleção para o exame da comunicação adquirida em larga escala. Além disso, um exame deliberado em violação destas salvaguardas constitui igualmente uma infração penal (ver a *section 173* do IPA 2016).

([408]) *Section 171* do IPA 2016.

([409]) *Section 171(9)* do IPA 2016.

([410]) *Section 162* do IPA 2016.

([411]) *Section 163* do IPA 2016.

([412]) *Section 164* a *166* do IPA 2016.

([413]) *Section 159* do IPA 2016.

(238) O comissário para os poderes de investigação procede a uma supervisão *ex post* do procedimento de exame do material (dados de comunicações) adquirido em larga escala (ver o considerando 254). A este respeito, o IPA 2016 introduziu o requisito segundo o qual o analista de informações que efetua o exame, antes de selecionar os dados para exame, deve registar a razão pela qual o exame proposto é necessário e proporcionado para uma finalidade operacional especificada ([414]). No relatório anual de 2019 do IPCO constatou-se, no que respeita à prática do GCHQ e do MI5, que o papel crucial dos dados de comunicações em larga escala para o conjunto de atividades realizadas no GCHQ estava bem articulado nos processos inspecionados. Considerou-se a natureza dos dados solicitados e os requisitos de informação declarados, tendo se considerado, de forma satisfatória, que a documentação demonstrava que a abordagem era necessária e proporcionada ([415]). As justificações registadas no MI5 eram de boa qualidade e satisfaziam os princípios da necessidade e da proporcionalidade ([416]).

3.3.1.1.4.3 Conservação e exame de conjuntos de dados pessoais em larga escala

(239) Os mandados de conjuntos de dados pessoais em larga escala ([417]) autorizam as agências de informações a conservar e a examinar conjuntos de dados que contenham dados pessoais relativos a várias pessoas. De acordo com as explicações prestadas pelas autoridades do Reino Unido, a análise desses conjuntos de dados pode constituir a única forma de a UKIC (comunidade dos serviços de informações do Reino Unido) fazer avançar investigações e identificar terroristas a partir de informações de base muito limitadas, ou quando as suas comunicações tenham sido deliberadamente ocultadas ([418]). Existem dois tipos de mandados: «mandados de conjuntos dados pessoais em larga escala de classe» ([419]), que dizem respeito a uma determinada categoria de conjuntos de dados, ou seja, conjuntos de dados que são semelhantes no seu conteúdo e na sua utilização proposta e que suscitam considerações semelhantes, por exemplo, quanto ao nível de intrusão e sensibilidade e à proporcionalidade da utilização dos dados, permitindo assim ao ministro da tutela ponderar, de uma só vez, a necessidade e a proporcionalidade de adquirir todos os dados dentro da classe em causa. Por exemplo, um mandado de conjuntos dados pessoais em larga escala de classe pode abranger conjuntos de dados de viagem relativos a rotas semelhantes ([420]). Por sua vez, os «mandados de conjuntos dados pessoais em larga escala específicos» ([421]) dizem respeito a um conjunto de dados específico, tais como um conjunto de dados de um tipo de informação novo ou invulgar que não se enquadra num mandado de conjuntos dados pessoais em larga escala de classe existente, ou um conjunto de dados que diz respeito a tipos específicos de dados pessoais ([422]), exigindo, por conseguinte, garantias adicionais ([423]). As disposições do IPA 2016 relativas aos conjuntos dados pessoais em larga escala permitem que esses conjuntos de dados sejam examinados e conservados apenas nos casos em que tal se mostre necessário e proporcionado ([424]) e em conformidade com as obrigações gerais em matéria de privacidade ([425]).

(240) O poder de emitir um mandado de conjuntos de dados pessoais em larga escala está sujeito ao procedimento de «dupla segurança»: a apreciação da necessidade e da proporcionalidade da medida é efetuada, em primeiro lugar, pelo ministro da tutela e, em seguida, pelo comissário judicial ([426]). O ministro da tutela está obrigado a ponderar a natureza e o alcance do tipo de mandado solicitado, a categoria dos dados em causa e o número de conjuntos de dados pessoais individuais suscetíveis de serem abrangidos pelo tipo específico de mandado ([427]). Além disso, tal como especificado no *Code of Practice on Intelligence Services' Retention and Use of Bulk Personal Datasets*, devem ser conservados registos pormenorizados e estes estão sujeitos a auditoria do comissário para os poderes de investigação ([428]). A conservação e o exame de conjuntos de dados pessoas em larga escala fora dos limites do IPA 2016 constitui uma infração penal ([429]).

([414]) Relatório anual de 2019 do IPCO, ponto 8.6, ver a nota de rodapé 463.
([415]) Relatório anual de 2019 do IPCO, ponto 10.4, ver a nota de rodapé 463.
([416]) Relatório anual de 2019 do IPCO, ponto 8.37, ver a nota de rodapé 463.
([417]) *Section 200* do IPA 2016.
([418]) *Explanatory Framework for Adequacy Discussions, section H: National security* (Secção H do quadro explicativo do Reino Unido para debates de adequação: segurança nacional), p. 34, ver a nota de rodapé 29.
([419]) *Section 204* do IPA 2016.
([420]) *Code of Practice on Intelligence Services' Retention and Use of Bulk Personal Datasets* (código de boas práticas sobre a conservação e utilização de conjuntos de dados pessoais em larga escala dos serviços de informações), ponto 4.7, disponível na seguinte ligação: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715478/Bulk_Personal_Datasets_Code_of_Practice.pdf
([421]) *Section 205* do IPA 2016.
([422]) Como, por exemplo, dados pessoais sensíveis, ver a *section 202* do IPA 2016 e o *Code of Practice on Intelligence Services' Retention and Use of Bulk Personal Datasets*, pontos 4.21 e 4.12, ver a nota de rodapé 469.
([423]) Um pedido de um mandado de conjuntos de dados pessoais em larga escala específicos deve ser analisado individualmente pelo ministro da tutela, ou seja, em relação a um conjunto de dados específico. O serviço de informações é obrigado, nos termos da *section 205* do IPA, a incluir no seu pedido de mandado de conjuntos de dados pessoais em larga escala específicos uma explicação pormenorizada da natureza e extensão do material em questão e uma lista das «finalidades operacionais» para as quais o serviço de informações pretende examinar o conjunto de dados pessoais em larga escala (quando o serviço de informações solicitar um mandado para conservação e exame e não apenas para conservação). Por sua vez, ao emitir um mandado de conjuntos de dados pessoais em larga escala de classe, o ministro da tutela tem imediatamente em conta toda a categoria de conjuntos de dados.
([424]) *Section 204* e *section 205* do IPA 2016.
([425]) *Section 2* do IPA 2016.
([426]) *Sections 204* e *205* do IPA 2016.
([427]) *Code of Practice on Intelligence Services' Retention and Use of Bulk Personal Datasets*, ponto 5.2, ver a nota de rodapé 420.
([428]) *Code of Practice on Intelligence Services' Retention and Use of Bulk Personal Datasets*, pontos 8.1 a 8.15, ver a nota de rodapé 420.
([429]) *Explanatory Framework for Adequacy Discussions, section H: National security* (Secção H do quadro explicativo do Reino Unido para debates de adequação: segurança nacional), p. 34, ver a nota de rodapé 29.

3.3.2 *Utilização adicional das informações recolhidas*

(241) Os dados pessoais tratados ao abrigo da parte 4 do DPA 2018 não podem ser tratados de forma incompatível com a finalidade para a qual foram recolhidos ([430]). O DPA 2018 prevê que o responsável pelo tratamento pode tratar os dados para outra finalidade, diferente daquela para a qual foram recolhidos, quando for compatível com a finalidade original e desde que o responsável pelo tratamento esteja autorizado por lei a tratar os dados e que o tratamento seja necessário e proporcionado ([431]). Além disso, o *Security Service Act 1989* e o *Intelligence Services Act 1994* especificam que os diretores dos serviços de informações têm o dever de assegurar que nenhuma informação seja obtida ou divulgada, exceto na medida do necessário para o correto exercício das funções da agência ou para outros fins limitados e específicos enumerados nas disposições pertinentes ([432]).

(242) Além disso, a *section 109* do DPA 2018 estabelece requisitos específicos para as transferências internacionais de dados pessoais pelos serviços de informações para países terceiros ou organizações internacionais. Nos termos desta disposição, os dados pessoais não podem ser transferidos para um país ou território fora do Reino Unido ou para uma organização internacional, a menos que a transferência seja necessária e proporcionada para o exercício das funções legais do responsável pelo tratamento ou para outras finalidades previstos na *section 2(2)(a)* do *Security Service Act 1989* ou nas *sections 2(2)(a)* e *4(2)(a)* do *Intelligence Services Act 1994* ([433]). Importa notar que estes requisitos são igualmente aplicáveis nos casos em que é invocada a isenção relativa à segurança nacional nos termos da *section 110* do DPA 2018, uma vez que a *section 110* do DPA de 2018 não enumera a *section 109* do DPA 2018 como uma das disposições que não são suscetíveis de aplicação se for necessária uma isenção de determinadas disposições para efeitos de garantia da segurança nacional.

(243) Além disso, tal como salientado pelo ICO nas suas orientações sobre o tratamento pelos serviços de informações, para além das garantias previstas na parte 4 do DPA 2018, uma agência de informações, quando partilha dados com um organismo de informações de um país terceiro, encontra-se igualmente sujeita às garantias previstas por outras medidas legislativas que lhes são aplicáveis, a fim de garantir que os dados pessoais são obtidos, partilhados e tratados de forma lícita e responsável ([434]). Por exemplo, o IPA 2016 estabelece salvaguardas adicionais em relação às transferências para um país terceiro de material recolhido através de interceção direcionada ([435]), interferência direcionada em equipamentos ([436]), interceção em larga escala ([437]), aquisição em larga escala de dados de comunicações ([438]) e interferência em equipamentos em larga escala ([439]) (as chamadas «divulgações no estrangeiro»). Em especial, a autoridade que emite o mandado deve assegurar que estão em vigor disposições para garantir que o país terceiro que recebe os dados limita ao mínimo necessário, para as finalidades autorizadas previstas no IPA 2016, o número de pessoas que veem o material, o âmbito da divulgação e o número de cópias de qualquer material ([440]).

3.3.3 *Supervisão*

(244) O acesso do governo para fins de segurança nacional é supervisionado por vários organismos diferentes. O comissário para a informação supervisiona o tratamento de dados pessoais à luz do DPA 2018 (para mais informações sobre a independência, a função de nomeação e os poderes do comissário, ver os considerandos 85 a 98), ao passo que a supervisão independente e judicial do uso de poderes de investigação ao abrigo do IPA 2016 é assegurado pelo comissário para os poderes de investigação. O comissário para os poderes de investigação

([430]) *Section 87(1)* do DPA 2018.

([431]) *Section 87(3)* do DPA 2018. Embora os responsáveis pelo tratamento possam estar isentos deste princípio nos termos da *section 110* do DPA 2018, na medida em que tal isenção seja necessária para salvaguardar a segurança nacional, essa isenção deve ser avaliada caso a caso e só pode ser invocada na medida em que a aplicação de uma disposição específica tenha consequências negativas para a segurança nacional (ver o considerando 132). Os certificados de segurança nacional para os serviços de informações do Reino Unido (disponíveis na seguinte ligação: https://ico.org.uk/about-the-ico/our-information/national-security-certificates/) não abrangem a *section 87(3)* do DPA 2018. Além disso, uma vez que qualquer tratamento com uma finalidade diferente deve ser autorizado por lei, os serviços de informações devem dispor de uma base jurídica clara para o tratamento posterior.

([432]) Para informações adicionais sobre estes fins, ver a nota de rodapé 312.

([433]) Ver a nota de rodapé 312.

([434]) Orientações do ICO sobre o tratamento pelos serviços de informações (ver a nota de rodapé 161).

([435]) *Section 54* do IPA 2016.

([436]) *Section 130* do IPA 2016.

([437]) *Section 151* do IPA 2016.

([438]) *Section 171(9)* do IPA 2016.

([439]) *Section 192* do IPA 2016.

([440]) As disposições devem incluir medidas destinadas a garantir que todas as cópias de qualquer um desses materiais são armazenadas de forma segura enquanto forem conservadas. O material obtido ao abrigo de um mandado e todas as cópias de qualquer desses materiais devem ser destruídos logo que deixem de existir motivos pertinentes para a sua conservação (ver *sections 150(2)*, *150(5)* e *151(2)* do IPA 2016). Importa notar que garantias semelhantes, previstas no quadro jurídico anterior (RIPA 2000), foram consideradas em conformidade com os requisitos estabelecidos pelo Tribunal Europeu dos Direitos Humanos para a partilha de material obtido por interceção em larga escala com Estados estrangeiros ou organizações internacionais (Tribunal Europeu dos Direitos Humanos (Grande Secção), *Big Brother Watch e o./Reino Unido* [ver a nota de rodapé 279 acima], n.os 362 e 399).

supervisiona o uso de poderes de investigação do IPA 2016 pelas autoridades responsáveis pela aplicação da lei e pelas autoridades de segurança nacional. A supervisão política é garantida pela *Intelligence Service Committee* (comissão para os serviços de informações) do parlamento.

3.3.3.1 Supervisão ao abrogo da parte 4 do DPA

(245) O tratamento de dados pessoais efetuado pelos serviços de informações ao abrigo da parte 4 do DPA 2018 é supervisionado pelo comissário para a informação ([441]).

(246) As funções gerais do comissário para a informação relativas ao tratamento de dados pessoais pelos serviços de informações ao abrigo da parte 4 do DPA 2018 são estabelecidas no *schedule 13* do DPA 2018. As funções incluem, nomeadamente, o acompanhamento e a aplicação coerciva da parte 4 do DPA 2018, a sensibilização do público, a prestação de aconselhamento ao parlamento, ao governo e a outras instituições em matéria de medidas legislativas e administrativas, a sensibilização dos responsáveis pelo tratamento e subcontratantes para as respetivas obrigações, a prestação de informações aos titulares dos dados relativamente ao exercício dos seus direitos, a realização de investigações, etc.

(247) No que respeita à parte 3 do DPA 2018, o comissário tem o poder de notificar os responsáveis pelo tratamento de uma alegada violação e avisar para a eventualidade de uma operação de tratamento poder violar as normas, emitindo repreensões caso se confirme a violação. Pode igualmente emitir notificações de execução e sanção por violação de determinadas disposições da lei ([442]). No entanto, ao contrário do que acontece noutras partes do DPA 2018, o comissário não pode proceder a uma notificação de avaliação a um organismo nacional de segurança ([443]).

(248) Além disso, a *section 110* do DPA 2018 prevê uma exceção ao uso de certos poderes do comissário sempre que tal seja necessário para efeitos de salvaguarda da segurança nacional. Tal inclui o poder conferido ao comissário para emitir (todos os tipos de) notificações abrangidas pelo DPA (notificações de informação, avaliação, execução e sanção), o poder de realizar inspeções em conformidade com as obrigações internacionais, os poderes de entrada e inspeção e as normas em matéria de infrações ([444]). Tal como explicado no considerando 126, estas exceções só se aplicam se forem necessárias e proporcionadas e numa base casuística.

(249) O comissário para a informação e os serviços de informações do Reino Unido assinaram um memorando de entendimento ([445]), que estabelece um quadro de cooperação referente a um conjunto de questões, incluindo as notificações de violações de dados e o tratamento das reclamações dos titulares dos dados. Nomeadamente, o referido quadro prevê que, ao receber uma reclamação, o comissário para a informação avaliará se a isenção de segurança nacional foi aplicada de forma correta. O serviço de informações em causa tem de responder às questões colocadas pelo comissário para a informação no âmbito da análise de reclamações individuais devem ser dadas no prazo de 20 dias úteis, utilizando para o efeito canais seguros adequados, caso envolvam informações confidenciais. Desde abril de 2018 até à data, o comissário para a informação recebeu 21 reclamações sobre os serviços de informações, tendo sido apreciada cada uma delas e o respetivo resultado comunicado ao titular dos dados ([446]).

([441]) *Section 116* do DPA 2018.

([442]) Nos termos do *schedule 13*, ponto 2, do DPA 2018, podem ser emitidas notificações de execução e sanção a um responsável pelo tratamento ou subcontratante em relação a violações da parte 4, capítulo 2, do DPA 2018 (princípios do tratamento), de uma disposição da parte 4 do DPA 2018 que confira direitos a um titular de dados, da obrigação de comunicar uma violação de dados pessoais ao comissário nos termos da *section 108* do DPA 2018, e dos princípios aplicáveis às transferências de dados pessoais para países terceiros, países que não sejam membros da Convenção e organizações internacionais da *section 109* do DPA (para mais informações sobre a notificação de execução e sanção, ver o considerando 92).

([443]) Nos termos da *section 147(6)* do DPA de 2018, o comissário para a informação não pode notificar um organismo especificado na *section 23(3)* do *Freedom of Information Act 2000* (Lei de 2000 relativa à Liberdade de Informação). Incluem-se aqui o *Security Service* (serviço de segurança) (MI5), o *Secret Intelligence Service* (serviço de informações secretas) (MI6) e o *Government Communications Headquarter* (quartel-general de comunicações do Estado).

([444]) As disposições passíveis de isenção são: *section 108* (comunicação de uma violação de dados pessoais ao comissário), *section 119* (inspeção em conformidade com as obrigações internacionais), *sections 142* a *154* e *schedule 15* (notificações do comissário e poderes de entrada e de inspeção) e *sections 170* a *173* (infrações relativas a dados pessoais). Além disso, em relação ao tratamento efetuado pelos serviços de informações previsto no *schedule 13* (outras funções gerais do comissário), n.º 1, alíneas a) e g), e n.º 2.

([445]) Memorando de entendimento celebrado entre o Gabinete do Comissário para a Informação e o *UK Intelligence Community*, ver a nota de rodapé 165.

([446]) Em sete destes casos, o comissário para a informação aconselhou o reclamante a dar a conhecer as suas preocupações ao responsável pelo tratamento (trata-se dos casos em que a pessoa deu a conhecer as suas preocupações ao comissário para a informação, mas deveria tê-lo feito primeiro junto do responsável pelo tratamento). Num dos casos, o comissário para a informação prestou aconselhamento geral ao responsável pelo tratamento (esta opção é utilizada quando não se afigura que os atos do responsável pelo tratamento tenham violado a legislação, mas uma melhoria das práticas poderia ter evitado que a questão fosse suscitada junto do comissário para a informação) e noutros 13 casos não foi necessária qualquer medida por parte do responsável pelo tratamento [esta opção é utilizada quando as questões suscitadas pelas pessoas são abrangidas pelo *Data Protection Act 2018*, uma vez que dizem respeito ao tratamento de informações pessoais, mas em que, com base nas informações transmitidas, não se afigura ter havido uma violação da legislação por parte do responsável pelo tratamento].

3.3.3.2 Supervisão do uso de poderes de investigação ao abrigo do IPA 2016

(250) Nos termos da parte 8 do IPA 2016, a supervisão do uso dos poderes de investigação é exercida pelo comissário para os poderes de investigação. Este comissário é assistido por outros comissários judiciais, coletivamente designados por «comissários judiciais» ([447]). O IPA 2016 estabelece as garantias que protegem a independência dos comissários judiciais. Os comissários judiciais são obrigados a exercer ou ter exercido um alto cargo judicial (ou seja, têm de ser ou de ter sido membros dos tribunais superiores) ([448]) e, como qualquer membro do poder judicial, gozam de um estatuto de independência do governo ([449]). Nos termos da *section 227* do IPA 2016, é o primeiro-ministro que nomeia o IPC e o número de comissários judiciais que considere necessários. Todos os comissários, quer sejam ou tenham sido magistrados, só podem ser nomeados com base numa recomendação conjunta dos três presidentes do sistema judiciário da Inglaterra, do País de Gales, da Escócia e da Irlanda do Norte e do Lorde Chanceler ([450]). O ministro da tutela deve fornecer ao comissário para os poderes de investigação pessoal, alojamento, equipamento e outras instalações e serviços ([451]). O mandato dos comissários é de três anos, podendo ser reconduzidos no cargo ([452]). Como garantia adicional da sua independência, os comissários judiciais só podem ser destituídos do cargo mediante condições estritas que impõem um limiar elevado: pelo primeiro-ministro, nas circunstâncias específicas enumeradas de forma exaustiva na *section 228(5)* do IPA 2016 (por exemplo, falência ou prisão), ou em caso de aprovação de uma resolução para a destituição por ambas as câmaras do parlamento britânico ([453]).

(251) O comissário para os poderes de investigação e os comissários judiciais são apoiados, nas suas funções, pelo IPCO. O pessoal do IPCO inclui uma equipa de inspetores, especialistas em assuntos jurídicos e técnicos internos e um painel consultivo tecnológico para prestar aconselhamento especializado. Dado ser o caso para os comissários judiciais a nível individual, a independência do IPCO está protegida. O IPCO é um organismo público independente do Ministério da Administração Interna britânico, ou seja, recebe financiamento deste ministério, mas desempenha as suas funções de forma independente ([454]).

(252) As principais funções dos comissários judiciais encontram-se descritas na *section 229* do IPA 2016 ([455]). Em especial, os comissários judiciais dispõem de um amplo poder de aprovação prévia, que faz parte das salvaguardas introduzidas no quadro jurídico do Reino Unido com o IPA 2016. Os mandados relativos a interceções direcionadas, interferências em equipamentos, conjuntos de dados pessoais em larga escala, aquisição em larga escala de dados de comunicações, bem como notificações de conservação de dados de comunicação, têm de ser aprovados pelos comissários judiciais ([456]). Além disso, o comissário para os poderes de investigação deve sempre autorizar previamente a aquisição de dados de comunicações para efeitos de aplicação da lei ([457]). Se um comissário se recusar a aprovar um mandado, o ministro da tutela pode recorrer para o comissário para os poderes de investigação, cuja decisão é definitiva.

([447]) Em conformidade com a *section 227(7)* e *(8)* do IPA 2016, o comissário para os poderes de investigação é um comissário judicial e comissário para os poderes de investigação e os outros comissários judiciais são conhecidos, coletivamente, como comissários judiciais. Existem atualmente 15 comissários judiciais.

([448]) Nos termos da *section 60(2)* da parte 3 do *Constitutional Reform Act 2005* (Lei de 2005 relativa à Reforma Constitucional), entende-se por «alto cargo judicial» o cargo de juiz de qualquer um dos seguintes tribunais: i) o *Supreme Court* (Supremo Tribunal), ii) o *Court of Appeal in England and Wales* (Tribunal de Recurso da Inglaterra e do País de Gales), iii) o *High Court in England and Wales* (Tribunal Superior da Inglaterra e do País de Gales), iv) o *Court of Session* (Tribunal de Sessão), v) o *Court of Appeal in Northern Ireland* (Tribunal de Recurso da Irlanda do Norte), vi) o *High Court in Northern Ireland* (Tribunal Superior da Irlanda do Norte); ou o cargo de *Lord of Appeal in Ordinary* (Lorde de Recurso Ordinário).

([449]) A independência do poder judicial baseia-se numa convenção e tem sido amplamente reconhecido desde o *1701 Act of Settlement* (Lei de 1701 relativa à Sucessão da Coroa).

([450]) *Section 227(3)* do IPA 2016. Os comissários judiciais devem também ser recomendados pelo comissário para os poderes de investigação, *section 227(4)(e)* do IPA 2016.

([451]) *Section 238* do IPA 2016.

([452]) *Section 227(2)* do IPA 2016.

([453]) O processo de destituição é idêntico ao processo de destituição para outros juízes no Reino Unido [ver, por exemplo, a *section 11(3)* do *Senior Courts Act 1981* (Lei de 1981 relativa aos Tribunais Superiores) e a *section 33* do *Constitutional Reform Act 2005*, que também exigem uma resolução na sequência de uma aprovação por ambas as câmaras do parlamento]. Até à data, nenhum comissário judicial foi destituído das suas funções.

([454]) Um organismo público independente é uma organização ou agência que recebe financiamento público, mas capaz de agir de forma independente (para uma definição e mais informações sobre um organismo público independente, consultar o manual do Gabinete de Ministros sobre a classificação dos organismos públicos, disponível na seguinte ligação: https://assets.publishing.service.gov.uk//government/uploads/system/uploads/attachment_data/file/519571/Classification-of-Public_Bodies-Guidance-for-Departments.pdf e o primeiro relatório da sessão de 2014-2015 da *Public Administration Select Committee* (comissão especial para a administração pública) da Câmara dos Comuns, disponível na seguinte ligação: https://publications.parliament.uk/pa/cm201415/cmselect//cmpubadm/110/110.pdf).

([455]) De acordo com a *section 229* do IPA 2016, o comissário judicial dispõe de amplos poderes de supervisão, que abrangem igualmente a supervisão da conservação e da divulgação dos dados recolhidos pelos serviços de informações.

([456]) Compete aos próprios comissários judiciais decidir quanto à aprovação de uma decisão do ministro da tutela de emitir um mandado. Se um comissário se recusar a aprovar um mandado, o ministro da tutela pode recorrer para o comissário para os poderes de investigação, cuja decisão é definitiva.

([457]) A autorização do comissário para os poderes de investigação é sempre solicitada quando os dados de comunicações são adquiridos para efeitos de aplicação da lei (*section 60A* do IPA 2016). Quando os dados de comunicações são adquiridos para efeitos de segurança nacional, a autorização pode ser concedida pelo comissário para os poderes de investigação ou, em alternativa, por um dirigente superior designado da autoridade pública competente (ver *sections 61* e *61A* do IPA 2016 e o considerando 203).

(253) O relator especial da ONU sobre o direito à privacidade saudou vivamente a criação dos comissários judiciais com o IPA 2016, uma vez que todos os pedidos mais sensíveis ou intrusivos para a realização de vigilância têm de ser autorizados tanto por um ministro como pelo Gabinete do Comissário para os Poderes de Investigação. Salientou, em especial, que este elemento de controlo judicial [através do papel da comissário para os poderes de investigação], assistido por uma equipa de inspetores experientes e peritos em tecnologia com melhores recursos, é uma das novas salvaguardas mais significativas introduzidas pelo IPA, substituindo um sistema anteriormente fragmentado de autoridades de supervisão e complementando o papel da *Intelligence and Security Committee* (comissão para a informação e a segurança) do parlamento e o *Investigatory Powers Tribunal* ([458]).

(254) Além disso, o comissário para os poderes de investigação tem poderes para efetuar uma supervisão *ex post*, incluindo por meio de uma auditoria, do uso dos poderes de investigação ao abrigo do IPA 2016 ([459]) e de outros poderes e funções previstos na legislação aplicável ([460]). Os resultados dessa supervisão *ex post* são incluídos no relatório que o comissário para os poderes de investigação deve elaborar anualmente e apresentar ao primeiro-ministro ([461]) e que deve ser publicado e apresentado ao parlamento ([462]). O relatório contém estatísticas e informações pertinentes sobre o uso dos poderes de investigação por parte dos serviços de informações e das autoridades responsáveis pela aplicação da lei, bem como sobre a utilização das salvaguardas em relação a elementos sujeitos à prerrogativa legal de confidencialidade, material jornalístico e fontes de informação jornalística confidenciais, informações sobre os mecanismos adotados e as finalidades operacionais utilizadas no contexto de mandados em larga escala. Por último, no relatório anual do IPCO, especifica-se em que domínio foram formuladas recomendações às autoridades públicas e como as mesmas foram abordadas ([463]).

(255) Em conformidade com a *section 231* do IPA 2016, se o comissário para os poderes de investigação tiver conhecimento de qualquer erro relevante cometido pelas autoridades públicas no exercício dos respetivos poderes de investigação, deve informar a pessoa em causa sempre que considere que o erro é grave e que é do interesse público que a pessoa seja informada ([464]). Em especial, a *section* 231 do IPA 2016 especifica que, ao informar uma pessoa de um erro, o comissário para os poderes de investigação deve fornecer informações sobre qualquer direito que tenha de requerer ao *Investigatory Powers Tribunal* e fornecer as informações que o comissário considere necessárias para o exercício desses direitos e da existência de um interesse público para a divulgação ([465]).

([458]) *End of Mission Statement of the Special Rapporteur on the Right to Privacy at the Conclusion Of his Mission to the United Kingdom of Great Britain and Northern Ireland* (ver a nota de rodapé 281).

([459]) *Section 229* do IPA 2016. Os poderes em matéria de investigação e de informação do comissário judicial encontram-se descritas na *section 235* do IPA 2016.

([460]) Tal inclui medidas de vigilância ao abrigo do RIPA 2000, o exercício de funções ao abrigo da parte 3 do *Police Act 1997* (Lei de 1997 relativa à Polícia) (autorização de ação em matéria de propriedade) e o exercício pelo ministro da tutela das funções ao abrigo das *sections 5* a *7* do *Intelligence Services Act 1994* (mandados de interferência em telegrafia sem fios, entrada e interferência em propriedade (*section 229* do IPA 2016).

([461]) *Section 230* do IPA 2016. O comissário para os poderes de investigação pode igualmente informar o primeiro-ministro, por sua iniciativa, sobre qualquer questão relacionada com as suas funções. O comissário para os poderes de investigação deve igualmente informar o primeiro-ministro, a seu pedido, e o este pode instruir o comissário para os poderes de investigação para rever todas as funções dos serviços de informações.

([462]) Algumas partes podem ser excluídas se a sua publicação for contrária à segurança nacional.

([463]) Por exemplo, no relatório anual de 2019 do IPCO (ponto 6.38), é referido que foi recomendado ao MI5 que alterasse a sua política de conservação de conjuntos de dados pessoais em larga escala, uma vez que deveria ter adotado uma abordagem em que fosse tida em conta a proporcionalidade da conservação para todos os domínios de detenção de conjuntos de dados pessoais em larga escala e relativamente a cada conjunto de dados pessoais em larga escala detido. No final de 2018, o IPCO não estava convencido de que esta recomendação tinha sido seguida e o relatório de 2019 explicava que a MI5 está agora a introduzir um novo procedimento para cumprir este requisito. O relatório anual de 2019 (ponto 8.22) refere igualmente que foram formuladas várias recomendações para o GCHQ relativas à contabilização dos registos da proporcionalidade das suas consultas sobre dados em larga escala. O relatório confirma que foram introduzidas melhorias neste domínio no final de 2018. *Annual Report of the Investigatory Powers Commissioner Office 2019* (Relatório anual de 2019 do Gabinete do Comissário para os Poderes de Investigação), disponível na seguinte ligação: https://www.ipco.org.uk/docs/IPC%20Annual%20Report%202019_Web%20Accessible%20version_final.pdf. Além disso, cada inspeção do IPCO a uma autoridade pública é concluída com um relatório apresentado à autoridade e inclui todas as recomendações decorrentes dessa inspeção. Em seguida, o IPCO inicia cada inspeção subsequente com uma análise das recomendações formuladas anteriormente a respeito da última inspeção e reflete no novo relatório de inspeção se as recomendações anteriores foram aplicadas ou adiadas.

([464]) Um erro é considerado «grave» quando o comissário considerar que causou prejuízos ou danos significativos à pessoa em causa [*section 231(2)* do IPA 2016]. Em 2018, foram comunicados 22 erros, dos quais oito foram considerados graves e resultaram em informações à pessoa em causa. Ver *Annual Report of the Investigatory Powers Commissioner Office 2018* (Relatório anual de 2018 do Gabinete do Comissário para os Poderes de Investigação), anexo C (consultar https://www.ipco.org.uk/docs/IPCO%20Annual%20Report%202018%20final.pdf). Em 2019, 14 erros foram considerados graves. Ver *Annual Report of the Investigatory Powers Commissioner Office 2019* (Relatório anual de 2019 do Gabinete do Comissário para os Poderes de Investigação), anexo C, ver a nota de rodapé 463.

([465]) A *section 231* do IPA 2016 especifica que, ao informar uma pessoa de um erro, o comissário para os poderes de investigação deve fornecer as informações que o comissário considere necessárias para o exercício desses direitos, tendo em conta, nomeadamente, em que medida a divulgação dos dados é contrária ao interesse público ou prejudicial à prevenção ou deteção da criminalidade grave, ao bem-estar económico do Reino Unido ou ao exercício continuado das funções de qualquer um dos serviços de informações.

3.3.3.3 Supervisão parlamentar dos serviços de informações

(256) A base jurídica para a supervisão parlamentar exercida pela *Intelligence and Security Committee* (ISC) consta do *Justice and Security Act 2013* (Lei de 2013 relativa à Justiça e à Segurança) (JSA 2013) ([466]), instrumento que cria a ISC como uma comissão do parlamento do Reino Unido. Desde 2013, a ISC tem sido dotada de cada vez mais poderes, incluindo a supervisão das atividades operacionais dos serviços de segurança. Nos termos da *section 2* do JSA 2013, a ISC tem por missão supervisionar as despesas, a administração, a política e as operações das agências nacionais de segurança. O JSA 2013 especifica que a ISC pode realizar investigações sobre matérias operacionais quando estas não digam respeito a operações em curso ([467]). O memorando de entendimento celebrado entre o primeiro-ministro e a ISC ([468]) especifica os elementos a ter em conta ao ponderar se uma atividade integra ou não uma operação em curso ([469]). O primeiro-ministro também pode solicitar que a ISC investigue operações em curso, podendo esta analisar informações transmitidas voluntariamente pelas agências.

(257) Nos termos do *schedule 1* do JSA 2013, a ISC pode pedir a divulgação de quaisquer informações aos responsáveis por qualquer dos três serviços de informações. A agência está obrigada à disponibilização destas informações, salvo em caso de veto por parte do ministro da tutela ([470]). De acordo com as explicações fornecidas pelas autoridades do Reino Unido, na prática, muito poucas informações são ocultadas à ISC ([471]).

(258) A ISC é composta por membros pertencentes a ambas as câmaras do parlamento e nomeados pelo primeiro-ministro após consulta o líder da oposição ([472]). A ISC está obrigada a apresentar um relatório anual ao parlamento sobre o exercício das respetivas funções, bem como outros relatórios que considere adequados ([473]). Além disso, a ISC tem o direito de receber trimestralmente a lista das finalidades operacionais utilizada para examinar o material obtido em larga escala ([474]). O primeiro-ministro partilha com a ISC cópias das investigações, inspeções ou auditorias do comissário para os poderes de investigação são partilhadas, se a questão dos relatórios for relevante para as competências legais da comissão ([475]). Por último, a comissão pode solicitar ao comissário para os poderes de investigação a realização de uma investigação e este deve informar a ISC da decisão de proceder ou não a essa investigação ([476]).

(259) A ISC também forneceu informações sobre o projeto de IPA 2016, que resultou num conjunto de alterações que se encontram agora refletidas no IPA 2016 ([477]). Em especial, a ISC recomendou o reforço das salvaguardas de privacidade através da introdução de um conjunto de salvaguardas de privacidade aplicáveis a todos os poderes de

([466]) Tal como explicado pelas autoridades do Reino Unido, o JSA aumentou as competências da ISC no sentido de incluir uma função na supervisão da comunidade dos serviços de informações, permitindo uma supervisão retrospetiva das atividades operacionais dos serviços em matérias de interesse nacional significativo.

([467]) *Section 2* do JSA 2013.

([468]) Memorando de entendimento entre o primeiro-ministro e a ISC, disponível na seguinte ligação: http://data.parliament.uk/DepositedPapers/Files/DEP2013-0415/AnnexA-JSBill-summaryofISCMoU.pdf

([469]) Memorando de entendimento entre o primeiro-ministro e a ISC, ponto 14, ver a nota de rodapé 468.

([470]) O ministro da tutela só pode vetar a divulgação da informação por dois motivos: a informação é sensível e não deve ser divulgada à ISC no interesse da segurança nacional ou trata-se de informação de tal natureza que, se o ministro da tutela fosse convidado a apresentá-la a uma comissão especial parlamentar da Câmara dos Comuns, o ministro da tutela ponderaria se tal seria adequado (por motivos não limitados à segurança nacional) (*schedule 1*, n.º 4, ponto 2, do JSA 2013).

([471]) *Explanatory Framework for Adequacy Discussions, section H: National security* (Secção H do quadro explicativo do Reino Unido para debates de adequação: segurança nacional), p. 43, ver a nota de rodapé 31.

([472]) *Section 1* do JSA 2013. Os ministros não são elegíveis como membros. Os mandato dos membros da ISC terá igual duração à legislatura do parlamento em que foram nomeados. Podem ser destituídos por resolução da Câmara pela qual foram nomeados, se deixarem de ser deputados do parlamento ou se passarem a ministros. Os membros podem também renunciar ao cargo.

([473]) Os relatórios e as declarações da comissão estão disponíveis em linha na seguinte ligação: https://isc.independent.gov.uk/publications/. Em 2015, a ISC publicou um relatório intitulado *Privacy and Security: A modern and transparent legal framework* (Privacidade e segurança: um quadro jurídico moderno e transparente) (ver: https://isc.independent.gov.uk/wp-content/uploads/2021/01/20150312_ISC_PSRptweb.pdf), no qual analisou o quadro jurídico para as técnicas de vigilância utilizadas pelos serviços de informações e formulou um conjunto de recomendações que foram então tidas em conta e integradas no projeto de Lei relativa aos Poderes de Investigação que se converteu em lei, o IPA 2016. A resposta do governo ao relatório sobre a privacidade e a segurança está disponível na seguinte ligação: https://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20151208_Privacy_and_Security_Government_Response.pdf

([474]) *Section 142*, *161* e *183* do IPA 2016.

([475]) *Section 234* do IPA 2016.

([476]) *Section 236* do IPA 2016.

([477]) *Intelligence and Security Committee of Parliament, Report on the draft Investigatory Powers Bill* (Relatório sobre o projeto de Lei relativa aos Poderes de Investigação), disponível na seguinte ligação: https://isc.independent.gov.uk/wp-content/uploads/2021/01/20160209_ISC_Rpt_IPBillweb.pdf

investigação ([478]). Sugeriu igualmente alterações às capacidades propostas no que respeita à interferência em equipamentos, aos conjuntos de dados pessoais em larga escala e aos dados de comunicações, e solicitou outras alterações específicas para reforçar as limitações e salvaguardas no uso de poderes de investigação ([479]).

3.3.4 *Recurso*

(260) No domínio do acesso governamental para efeitos de segurança nacional, os titulares dos dados devem dispor da possibilidade de recorrer a medidas jurídicas corretivas eficazes num tribunal independente e imparcial, para ter acesso a dados pessoais que lhes digam respeito ou para obter a retificação ou a supressão desses dados ([480]). Tal órgão judicial deve, nomeadamente, estar habilitado a adotar decisões vinculativas para os serviços de informações ([481]). No Reino Unido, conforme explicado nos considerandos 261 a 271, há várias vias de recurso judicial que oferecem aos titulares dos dados a possibilidade de recorrer e aceder a medidas jurídicas corretivas.

3.3.4.1 Mecanismos de recurso disponíveis ao abrigo da parte 4 do DPA

(261) Ao abrigo da *section 165* do DPA 2018, um titular dos dados tem o direito de apresentar uma reclamação ao comissário para a informação caso considere que existe uma violação da parte 4 do DPA 2018 relacionada com dados pessoais que lhe digam respeito. O comissário para a informação está habilitado a avaliar o cumprimento do DPA 2018 por parte do responsável pelo tratamento e do subcontratante, e de exigir que estes tomem as medidas necessárias. Além disso, ao abrigo da parte 4 do DPA 2018, as pessoas singulares têm o direito de solicitar ao *High Court* [ou ao *Court of Session* (Tribunal de Sessão) na Escócia] que ordene ao responsável pelo tratamento que cumpra os direitos de acesso aos dados ([482]), de oposição ao tratamento ([483]) e de retificação ou apagamento ([484]).

(262) As pessoas singulares também têm o direito de pedir uma indemnização ao responsável pelo tratamento ou a um subcontratante por danos sofridos devido a uma violação de um requisito da parte 4 do DPA 2018 ([485]). Os danos incluem perdas financeiras e não financeiras, como sofrimento emocional ([486]).

3.3.4.2. Mecanismos de recurso previstos no IPA 2016

(263) As pessoas singulares podem obter reparação por violações do IPA 2016 junto do *Investigatory Powers Tribunal*.

(264) O *Investigatory Powers Tribunal* foi criado pelo RIPA 2000 e é independente do executivo ([487]). Nos termos da *section 65* do RIPA 2000, os seus membros são nomeados por Sua Majestade por um período de cinco anos, podendo ser afastados do cargo por Sua Majestade na sequência de um comunicado ([488]) de ambas as câmaras do parlamento ([489]).

([478]) Estes deveres gerais em matéria de privacidade encontram-se agora previstos na *section 2(2)* do IPA 2016, que prevê que uma autoridade pública, que atue ao abrigo do IPA 2016, deve ter em conta 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, 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, ao interesse público na integridade e segurança de quaisquer outros sistemas de telecomunicações e serviços postais, e a quaisquer outros aspetos de interesse público na proteção da privacidade.

([479]) Por exemplo, na sequência do pedido da ISC, foi reduzido de cinco para três dias o número de dias em que um mandado «urgente» pode estar em vigor antes de o comissário judicial o ter de aprovar, tendo sido conferido à ISC o poder de reencaminhar questões para investigação ao comissário para os poderes de investigação.

([480]) *Schrems II*, n.º 194.

([481]) *Schrems II*, n.º 197.

([482]) *Section 94(11)* do DPA 2018.

([483]) *Section 99(4)* do DPA 2018.

([484]) *Section 100(1)* do DPA 2018.

([485]) A *section 169* do DPA 2018 permite pedidos de indemnização de «[u]ma pessoa que sofra danos devido a uma violação de um requisito da legislação em matéria de proteção de dados». De acordo com as informações fornecidas pelas autoridades do Reino Unido, na prática, uma ação ou uma reclamação contra os serviços de informações serão provavelmente apresentadas no *Investigatory Powers Tribunal*, que tem uma ampla competência, pode atribuir indemnizações/compensações, e onde intentar uma ação não envolve custos.

([486]) *Section 169(5)* do DPA 2018.

([487]) Nos termos do *schedule 3* do RIPA 2000, os membros do tribunal devem ter experiência judicial especificada e são elegíveis para uma nova nomeação.

([488]) Um «comunicado» é uma moção apresentada ao parlamento que procura informar a monarca dos pareceres do parlamento numa determinada questão.

([489]) *Schedule 3*, n.º 1, ponto 5, do RIPA 2000.

(265) Nos termos da *section 65* do RIPA 2000, o tribunal é o órgão judicial adequado para qualquer reclamação apresentada por uma pessoa lesada por uma conduta no âmbito do IPA 2016, do RIPA 2000 ou por qualquer conduta dos serviços de informações ([490]).

(266) Para intentar uma ação no *Investigatory Powers Tribunal* («requisito de legitimidade»), nos termos da *section 65* do RIPA 2000, uma pessoa singular tem de estar convicta ([491]) de que a conduta de um serviço de informações teve lugar em relação a si, a qualquer um dos seus bens, a quaisquer comunicações por si enviadas, ou a si destinadas, ou à sua utilização de qualquer serviço postal, serviço de telecomunicações ou sistema de telecomunicações ([492]). Além disso, o autor da reclamação tem de estar convicto de que a conduta teve lugar em «circunstâncias contestáveis» ([493]) ou que «foi efetuada por ou em nome dos serviços de informações» ([494]). Como, em particular, este conceito de «convicção» tem sido interpretado de forma bastante ampla ([495]), recorrer a este tribunal está sujeito a baixos requisitos de legitimidade.

(267) Quando o *Investigatory Powers Tribunal* considera uma reclamação que lhe foi apresentada, deve investigar se as pessoas contra as quais é feita qualquer alegação na reclamação estiveram envolvidas no que respeita ao autor da reclamação, bem como investigar a autoridade que alegadamente esteve envolvida nas violações e se a alegada conduta teve lugar ([496]). Quando aprecia um processo, para proceder à sua determinação, o tribunal tem de aplicar os mesmos princípios que seriam aplicados por um tribunal num pedido de fiscalização jurisdicional ([497]). Além disso, os destinatários dos mandados ou notificações ao abrigo do IPA 2016, e qualquer funcionário da Coroa, da força policial ou do comissário para as investigações e análise da polícia (*Police Investigations and Review Commissioner*), têm o dever de revelar ou fornecer a esse tribunal todos os documentos e informações que o tribunal possa exigir para exercer a sua competência ([498]).

(268) O *Investigatory Powers Tribunal* tem de notificar o autor da reclamação se houve ou não determinação a seu favor ([499]). Ao abrigo da *section 67(6)* e *(7)* do RIPA 2000, o tribunal tem competência para adotar medidas provisórias e para conceder uma indemnização ou decretar outra medida que considere adequada. Tal pode incluir a anulação ou o cancelamento de qualquer mandado ou autorização e uma ordem que exija a destruição de quaisquer registos de informações obtidas no exercício de qualquer poder conferido por um mandado, uma autorização ou uma

([490]) *Section 65(5)* do RIPA 2000.

([491]) Sobre o critério de «convicção», ver o processo *Human Rights Watch/Secretary of State* [2016] UKIPTrib15_165-CH, n.º 41. Neste processo, o *Investigatory Powers Tribunal*, referindo-se à jurisprudência do Tribunal Europeu dos Direitos Humanos, considerou que o critério adequado, relativamente à convicção declarada de que uma conduta abrangida pela *subsection 68(5)* do RIPA 2000 foi levada a cabo por ou em nome de qualquer um dos serviços de informações, é se existe algum fundamento para tal convicção, de tal forma que a pessoa só possa alegar ser vítima de uma violação ocasionada pela mera existência de medidas secretas ou legislação que permita medidas secretas, se puder demonstrar que, devido à sua situação pessoal, está potencialmente em risco de ser sujeita a tais medidas.

([492]) *Section 65(4)(a)* do RIPA 2000.

([493]) Tais circunstâncias dizem respeito à conduta das autoridades públicas que tem lugar com autoridade (por exemplo, um mandado, uma autorização/notificação para a aquisição de comunicações, etc.), ou se as circunstâncias forem tais (exista ou não essa autoridade) que não teria sido adequado que a conduta tivesse ocorrido sem ela, ou pelo menos sem ter sido dada a devida consideração se tal autoridade deveria ser solicitada. As condutas autorizadas por um comissário judicial são consideradas como tendo ocorrido em circunstâncias contestáveis [*section 65 (7ZA)* do RIPA 2000], enquanto outras condutas que têm lugar com a autorização de uma pessoa que detém um cargo judicial são consideradas como não tendo ocorrido em circunstâncias contestáveis [*section 65(7)* e *(8)* do RIPA 2000].

([494]) De acordo com as informações fornecidas pelas autoridades do Reino Unido, o baixo limiar para a apresentação de uma reclamação faz com que não seja raro a investigação do tribunal determinar que o autor da reclamação nunca foi, na verdade, objeto de investigação por uma autoridade pública. O último relatório estatístico do *Investigatory Powers Tribunal* especifica que, em 2016, o tribunal recebeu 209 reclamações, 52% das quais foram consideradas levianas ou vexatórias e 25% receberam um resultado «sem determinação». As autoridades do Reino Unido explicaram que tal significa que não foram utilizados poderes/atividades encobertas em relação aos autores das reclamações, ou que foram utilizadas técnicas encobertas e que o tribunal determinou que a atividade era legal. Além disso, 11% foram consideradas como estando fora da sua competência, foram retiradas ou não eram válidas, 5% foram consideradas intempestivas, e 7% foram decididas a favor do autor da reclamação. Relatório estatístico do *Investigatory Powers Tribunal* de 2016, disponível na seguinte ligação: https://www.ipt-uk.com/docs/IPT%20Statisical%20Report%202016.pdf

([495]) Ver o processo *Human Rights Watch/Secretary of State* [2016] UKIPTrib15_165-CH. Neste processo, o *Investigatory Powers Tribunal*, referindo-se à jurisprudência do Tribunal Europeu dos Direitos Humanos, considerou que o critério adequado relativamente à convicção de que uma conduta abrangida pela *subsection 68(5)* do RIPA 2000 foi levada a cabo por ou em nome de qualquer um dos serviços de informações é se existe algum fundamento para tal convicção, incluindo o facto de uma pessoa só poder alegar ser vítima de uma violação ocasionada pela mera existência de medidas secretas ou legislação que permita medidas secretas, se puder demonstrar que, devido à sua situação pessoal, está potencialmente em risco de ser sujeita a tais medidas (ver *Human Rights Watch/Secretary of State*, n.º 41).

([496]) *Section 67(3)* do RIPA 2000.

([497]) *Section 67(2)* do RIPA 2000.

([498]) *Section 68(6)* – *(7)* do RIPA 2000.

([499]) *Section 68(4)* do RIPA 2000.

notificação, ou de outra forma detidas por qualquer autoridade pública relativamente a qualquer pessoa ([500]). De acordo com a *section 67A* do RIPA 2000, uma determinação do tribunal pode ser objeto de recurso, sob reserva de uma autorização concedida pelo tribunal ou pelo tribunal de recurso competente.

(269) Por último, deve salientar-se que o papel do *Investigatory Powers Tribunal* foi debatido no contexto de ações judiciais no Tribunal Europeu dos Direitos Humanos em várias ocasiões, nomeadamente no processo *Kennedy/Reino Unido* ([501]) e, mais recentemente, no processo *Big Brother Watch e o./Reino Unido* ([502]), em que o tribunal declarou que «o IPT proporcionou um recurso judicial sólido para qualquer pessoa que suspeite que as suas comunicações foram intercetadas pelos serviços de informações» ([503]).

3.3.4.3 Outros mecanismos de recurso disponíveis

(270) Conforme explicado nos considerandos 109 a 111, também estão disponíveis vias de recurso ao abrigo do *Human Rights Act 1998* e junto do Tribunal Europeu dos Direitos Humanos ([504]) no domínio da segurança nacional. A *section 65(2)* do RIPA 2000 concede ao *Investigatory Powers Tribunal* competência exclusiva para todas as reclamações ao abrigo do *Human Rights Act* relacionadas com os serviços de informações ([505]). Tal significa, conforme referido pelo *High Court*, que «a questão de ter havido uma violação do HRA no que respeita aos factos de um determinado caso é algo que pode, em princípio, ser suscitado e decidido por um tribunal independente, que pode ter acesso a todo o material pertinente, incluindo material secreto. [...] Neste contexto, temos também em mente que o tribunal está agora sujeito à possibilidade de recurso num tribunal de recurso competente (na Inglaterra e no País de Gales, *Court of Appeal*); e que o *Supreme Court* decidiu recentemente que o tribunal é, em princípio, passível de fiscalização jurisdicional: ver *R (Privacy International)/Investigatory Powers Tribunal* [2019] UKSC 22; [2019] 2 WLR 1219» ([506]).

(271) Decorre do acima exposto que quando as autoridades do Reino Unido responsáveis pela aplicação da lei ou pela segurança nacional acedem a dados pessoais abrangidos pela presente decisão, tal acesso é regido por leis que estabelecem as condições em que esse acesso pode ter lugar e garante que o acesso e a posterior utilização dos dados são limitados ao necessário e proporcionado para o objetivo de aplicação da lei ou de segurança nacional visado. Além disso, tal acesso está sujeito, na maioria dos casos, a uma autorização prévia da parte de uma autoridade judicial, através da aprovação de um mandado ou de uma ordem de entrega e, em qualquer caso, a um controlo independente. Assim que as autoridades públicas têm acesso aos dados, o seu tratamento, incluindo a partilha e posterior transferência, está sujeito a garantias específicas em matéria de proteção de dados ao abrigo da parte 3 do DPA 2018, que refletem as previstas na Diretiva (UE) 2016/680, para o tratamento pelas autoridades de aplicação da lei, e da parte 4 do DPA 2018, para o tratamento pelos serviços de informações. Por último, os titulares dos dados gozam, neste domínio, de direitos efetivos de recurso administrativo e judicial, incluindo a obtenção de acesso aos seus dados ou a retificação ou apagamento de tais dados.

(272) Dada a importância de tais condições, limitações e garantias para efeitos da presente decisão, a Comissão acompanhará de perto a aplicação e a interpretação das regras do Reino Unido que enquadram o acesso governamental aos dados. Tal incluirá desenvolvimentos legislativos, regulamentares e jurisprudenciais relevantes,

([500]) Um exemplo da aplicação dessas competências é o processo *Liberty e o./Security Service, SIS, GCHQ*, [2015] UKIP Trib 13_77-H_2. O tribunal decidiu a favor de dois autores de reclamações porque a sua comunicação, num caso, foi conservada além dos limites estabelecidos e, no outro, porque o procedimento de exame não foi seguido, conforme estabelecido no regulamento interno do GCHQ. No primeiro caso, o tribunal ordenou aos serviços de informações que destruíssem as comunicações que foram conservada por mais tempo do que o prazo pertinente. No segundo, não foi decretada uma ordem de destruição porque a comunicação não foi conservada.

([501]) *Kennedy*, ver nota de rodapé 129.

([502]) Tribunal Europeu dos Direitos Humanos, *Big Brother Watch e o./Reino Unido*, (ver a nota de rodapé 268 acima), n.os 413 a 415.

([503]) Tribunal Europeu dos Direitos Humanos, *Big Brother Watch*, n.º 425.

([504]) Tal como ilustrado, por exemplo, no recente acórdão da Grande Secção do Tribunal Europeu dos Direitos Humanos, no processo *Big Brother Watch e o./Reino Unido* (ver a nota de rodapé 279 acima), tal permite um controlo judicial efetivo — semelhante àquele a que os Estados-Membros da UE estão sujeitos — por um tribunal internacional sobre a conformidade com os direitos fundamentais por parte das autoridades públicas no acesso aos dados pessoais. Além disso, a execução dos acórdãos do Tribunal Europeu dos Direitos Humanos está sujeita a um controlo específico pelo Conselho da Europa.

([505]) No processo *Belhaj e o.* [2017] UKSC 3, a determinação da ilegalidade da interceção de material protegido pela confidencialidade baseou-se diretamente no artigo 8.º da CEDH (ver determinação 11).

([506]) *High Court of Justice, Liberty*, [2019] EWHC 2057 (Admin.), n.º 170.

bem como as atividades do ICO e de outras autoridades de supervisão neste domínio. Será também prestada especial atenção à execução pelo Reino Unido de acórdãos pertinentes do Tribunal Europeu dos Direitos Humanos, incluindo as medidas identificadas nos «planos de ação» e nos «relatórios de ação» apresentados ao Comité de Ministros no contexto do controlo da conformidade com as decisões do tribunal.

4. **CONCLUSÃO**

(273) A Comissão entende que o RGPD do Reino Unido e o DPA 2018 asseguram um nível de proteção dos dados pessoais transferidos da União Europeia essencialmente equivalente ao garantido pelo Regulamento (UE) 2016/679.

(274) Além disso, a Comissão considera que os mecanismos de controlo e as vias de recurso previstos na legislação do Reino Unido permitem, 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 apagamento dos mesmos.

(275) 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, será limitada ao estritamente necessário para alcançar o objetivo legítimo em causa, existindo uma proteção jurídica eficaz contra tal ingerência.

(276) Assim, atendendo às constatações efetuadas na presente decisão, deve decidir-se que o Reino Unido garante 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.

(277) Esta conclusão baseia-se tanto no regime interno aplicável do Reino Unido como nos seus compromissos internacionais, em particular a 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.

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

(278) 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.

(279) 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 particular, durante o período de aplicação da presente decisão, as transferências de um responsável pelo tratamento de dados ou de um subcontratante na União Europeia para responsáveis pelo tratamento e subcontratantes no Reino Unido podem ser efetuadas sem que seja necessária mais nenhuma autorização.

(280) 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 ([507]), 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 ([508]).

([507]) *Schrems*, n.º 65.

([508]) *Schrems*, 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».

6. ACOMPANHAMENTO, SUSPENSÃO, REVOGAÇÃO OU ALTERAÇÃO DA PRESENTE DECISÃO

(281) 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 após a adoção da presente decisão, a fim de avaliar se esta ainda assegura um nível de proteção essencialmente equivalente. Tal controlo é particularmente importante neste caso, uma vez que o Reino Unido administrará, aplicará e fará cumprir um novo regime de proteção de dados que já não estará sujeito ao direito da União Europeia e que pode ser suscetível de evoluir. A este respeito, será 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 presente decisão; à eficácia do exercício dos direitos individuais, incluindo qualquer desenvolvimento pertinente da legislação e das práticas relativas às exceções ou às restrições a tais 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 acompanhamento pela Comissão basear-se-á nos desenvolvimentos da jurisprudência e na supervisão pelo ICO e outros organismos independentes.

(282) A fim de facilitar este acompanhamento, 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 presente decisão, bem como de qualquer evolução das práticas relacionadas com o tratamento dos dados pessoais avaliadas na 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 281.

(283) 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.

(284) Sempre que as informações disponíveis, nomeadamente as resultantes do controlo da 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.

(285) 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.

(286) 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.

(287) 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. DURAÇÃO E RENOVAÇÃO DA PRESENTE DECISÃO

(288) A Comissão tem de ter em conta que, com o fim do período de transição previsto pelo Acordo de Saída, e logo que a disposição provisória constante do artigo 782.º do Acordo de Comércio e Cooperação UE-Reino Unido deixe de ser aplicável, o Reino Unido administrará, aplicará e fará cumprir um novo regime de proteção de dados em comparação com o que estava em vigor quando estava vinculado pelo direito da UE. Tal pode envolver, nomeadamente, alterações ou modificações do quadro de proteção de dados avaliado na presente decisão, bem como outros desenvolvimentos pertinentes.

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

(290) 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**

(291) O Comité Europeu para a Proteção de Dados publicou o seu parecer ([509]), que foi tido em conta na elaboração da presente decisão.

(292) As medidas previstas na presente decisão estão em conformidade com o parecer do Comité instituído ao abrigo do artigo 93.º do Regulamento (UE) 2016/679,

ADOTOU A PRESENTE DECISÃO:

Artigo 1.º

1. Para efeitos do artigo 45.º do Regulamento (UE) 2016/679, o Reino Unido assegura um nível adequado de proteção dos dados pessoais transferidos no âmbito do Regulamento (UE) 2016/679 da União Europeia para o Reino Unido.

2. A presente decisão não abrange os 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, nos termos do *schedule 2*, n.º 4, ponto 1, do DPA 2018.

Artigo 2.º

Sempre que, para efeitos de proteção das pessoas singulares no que se refere ao tratamento dos seus dados pessoais, as autoridades de controlo competentes dos Estados-Membros exercerem as suas competências, nos termos do artigo 58.º do Regulamento (UE) 2016/679 no que respeita às transferências de dados abrangidas pelo âmbito de aplicação previsto no artigo 1.º, o Estado-Membro em causa deve informar de imediato a Comissão.

Artigo 3.º

1. A Comissão deve garantir o controlo contínuo da aplicação do quadro jurídico em que assenta a presente decisão, nomeadamente as condições em que se procede a transferências ulteriores, o exercício dos direitos fundamentais e o acesso das autoridades públicas do Reino Unido a dados transferidos com base na presente decisão, por forma a avaliar se o Reino Unido continua a assegurar um nível de proteção adequado na aceção do artigo 1.º.

2. Os Estados-Membros e a Comissão devem comunicar-se reciprocamente os casos em que o comissário para a informação, ou qualquer outra autoridade competente do Reino Unido, deixe de cumprir o quadro jurídico em que a presente decisão assenta.

3. Os Estados-Membros e a Comissão devem comunicar-se reciprocamente quaisquer informações relativas a indícios de que a ingerência das autoridades públicas do Reino Unido no direito das pessoas singulares à proteção dos dados pessoais excede o estritamente necessário ou de que não existe uma proteção jurídica eficaz contra tal ingerência.

4. Se tomar conhecimento de quaisquer indícios de que deixou de ser assegurado um nível de proteção adequado, a Comissão deve informar desse facto as autoridades competentes do Reino Unido e pode suspender, revogar ou alterar a presente decisão.

([509]) Parecer 14/2021 sobre o projeto de decisão de execução da Comissão Europeia nos termos do Regulamento (UE) 2016/679 relativa à adequação do nível de proteção de dados pessoais no Reino Unido, disponível na seguinte ligação: https://edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-142021-regarding-european-commission-draft_en

5. A Comissão pode suspender, revogar ou alterar a presente decisão se a falta de cooperação do Governo do Reino Unido a impedir de determinar se a verificação prevista no artigo 1.º, n.º 1, foi afetada.

Artigo 4.º

A presente decisão caduca em 27 de junho de 2025, a menos que seja prorrogada nos termos do procedimento referido no artigo 93.º, n.º 2, do Regulamento (UE) 2016/679.

Artigo 5.º

Os destinatários da presente decisão são os Estados-Membros.

Feito em Bruxelas, em 28 de junho de 2021.

Pela Comissão
Didier REYNDERS
Membro da Comissão