DECISÃO DE EXECUÇÃO (UE) 2021/1773 DA COMISSÃO

de 28 de junho de 2021

nos termos da Diretiva (UE) 2016/680 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) 4801]

A COMISSÃO EUROPEIA,

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

Tendo em conta a Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho ([1]), nomeadamente o artigo 36.º, n.º 3,

Considerando o seguinte:

1. **INTRODUÇÃO**

(1) A Diretiva (UE) 2016/680 estabelece as regras relativas às transferências de dados pessoais pelas autoridades competentes na União para países terceiros e organizações internacionais, na medida em que essas transferências sejam abrangidas pelo respetivo âmbito de aplicação. As regras relativas às transferências internacionais de dados pelas autoridades competentes são estabelecidas no capítulo V da Diretiva (UE) 2016/680, mais especificamente nos seus artigos 35.º a 40.°. Embora a circulação de dados pessoais com destino e a partir de países fora da União Europeia seja essencial para uma cooperação eficiente no domínio da aplicação da lei, é indispensável garantir que o nível de proteção concedido aos dados pessoais na União Europeia não é prejudicado por tais transferências ([2]).

(2) Nos termos do artigo 36.º, n.º 3, da Diretiva (UE) 2016/680, a Comissão pode decidir, por meio de um ato de execução, que um país terceiro, um território, um ou mais setores específicos desse país terceiro, ou uma organização internacional, assegura(m) um nível de proteção adequado. Tendo em conta esta condição, pode-se efetuar transferências de dados pessoais para um país terceiro sem que seja necessária mais nenhuma autorização (salvo se outro Estado-Membro de onde provêm os dados tiver de autorizar a transferência), como previsto no artigo 35.º, n.º 1, e no considerando 66 da Diretiva (UE) 2016/680.

(3) Conforme especificado no artigo 36.º, n.º 2, da Diretiva (UE) 2016/680, a adoção de uma decisão de adequação tem de basear-se numa análise exaustiva da ordem jurídica do país terceiro. 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 67 da Diretiva (UE) 2016/680]. O critério pelo qual se avalia a «equivalência essencial» é o estabelecido pela legislação da UE, nomeadamente a Diretiva (UE) 2016/680, 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 é também importante nesta matéria ([4]).

(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, o padrão de adequação não exige que as regras da União sejam replicadas ponto por ponto. Em vez disso, importa aferir sobretudo se, por meio do teor dos direitos de privacidade e da sua aplicação, controlo e execução efetivos, o sistema estrangeiro consegue, no seu conjunto, garantir o nível de proteção exigido ([7]).

([1]) JO L 119 de 4.5.2016, p. 89.

([2]) Ver considerando 64 da Diretiva (UE) 2016/680.

([3]) Ver, mais recentemente, o processo C-311/18, Maximilian Schrems/Data Protection Commissioner («Schrems II») ECLI:EU:C:2020:559.

([4]) Ver *Recommendations 01/2021 on the adequacy referential under the Law Enforcement Directive* (Recomendações 01/2021 a respeito do documento de referência relativo à adequação nos termos da Diretiva Proteção de Dados na Aplicação da Lei), adotadas em fevereiro de 2021, disponíveis na seguinte ligação: https://edpb.europa.eu/our-work-tools/general-guidance/police-justice-guidelines--recommendations-best-practices_pt

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

([6]) Schrems, 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

(5) A Comissão analisou com atenção o direito e as práticas pertinentes do Reino Unido. Com base nas suas conclusões, expostas a abaixo, a Comissão conclui que o Reino Unido assegura um nível adequado de proteção dos dados pessoais transferidos pelas autoridades competentes na União, abrangidas pelo âmbito de aplicação da Diretiva (UE) 2016/680, às autoridades competentes do Reino Unido abrangidas pelo âmbito de aplicação da parte 3 do *Data Protection Act 2018* (Lei de 2018 relativa à Proteção de Dados – DPA 2018) ([8]).

(6) Em resultado da presente decisão, tais transferências podem ser efetuadas sem que seja necessária mais nenhuma autorização por um período de quatro anos, sob reserva de uma possível renovação e sem prejuízo das condições previstas no artigo 35.º da Diretiva (UE) 2016/680.

2. NORMAS APLICÁVEIS AO TRATAMENTO DE DADOS PESSOAIS POR AUTORIDADES COMPETENTES PARA FINS DE APLICAÇÃO DO DIREITO PENAL

2.1. Quadro constitucional

(7) O Reino Unido é uma democracia parlamentar. Possui um parlamento soberano, que tem supremacia em relação a todas as outras instituições governamentais, um executivo proveniente do parlamento e responsável perante este e um sistema judiciário independente. O executivo retira a sua autoridade da sua capacidade de congregar o apoio da Câmara dos Comuns eleita e é responsável perante ambas as câmaras do parlamento (Câmara dos Comuns e Câmara dos Lordes), que são responsáveis pelo controlo do governo e por debater e aprovar a legislação. 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 em certas matérias internas na Escócia, no País de Gales e na Irlanda do Norte. Embora a proteção de dados seja uma matéria reservada ao parlamento do Reino Unido, ou seja, é aplicável a mesma legislação a todo o território, existem outros domínios políticos pertinentes para a presente decisão que foram delegados. Por exemplo, os sistemas de justiça penal, incluindo o policiamento (as atividades realizadas pelas forças policiais) da Escócia e da Irlanda do Norte, são da competência do parlamento escocês e da Assembleia da Irlanda do Norte, respetivamente ([9]).

(8) Embora o Reino Unido não possua uma constituição codificada na aceção de um documento constitutivo codificado, os seus princípios constitucionais têm surgido com o passar do tempo, tendo origem, em particular, na jurisprudência e em convenções. Tem sido reconhecido o valor constitucional de determinadas leis, como a *Magna Carta*, o *Bill of Rights 1689* (Carta dos Direitos de 1689) e o *Human Rights Act 1998* (Lei de 1998 relativa aos Direitos Humanos). Os direitos fundamentais das pessoas singulares têm-se desenvolvido, como parte da constituição, por meio da jurisprudência, da legislação 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]).

(9) O *Human Rights Act 1998* incorpora os direitos constantes da CEDH no direito do Reino Unido. A referida lei concede a todas as pessoas os direitos e as liberdades fundamentais previstas nos artigos 2.º a 12.° e no artigo 14.º da CEDH, nos artigos 1.º a 3.° do seu Protocolo n.º 1 e no artigo 1.º do seu Protocolo n.º 13, lido em conjugação com os artigos 16.º a 18.° da CEDH. Tal inclui o direito ao respeito pela vida privada e familiar, que, por sua vez, inclui o direito à proteção dos dados, e o direito a um tribunal imparcial ([11]). Mais particularmente, nos termos do artigo 8.º da CEDH, só pode haver ingerência da autoridade pública se esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para 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.

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

([9]) *UK Explanatory Framework for Adequacy Discussions, Section F: Law enforcement*, (Quadro explicativo do Reino Unido para as conversações em matéria de adequação, secção F: Aplicação da lei), disponível na seguinte ligação: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872237/F_-_Law_Enforcement_.pdf

([10]) Os princípios da Convenção 108 foram inicialmente integrados no direito do Reino Unido por meio do *Data Protection Act of 1984* (Lei de 1984 relativa à Proteção de Dados), que foi substituído pelo DPA 1998, que, 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.° da CEDH (ver igualmente *schedule 1* do *Human Rights Act 1998*).

(10) Em conformidade com o *Human Rights Act 1998*, qualquer ato por parte das autoridades públicas tem de ser compatível com os direitos garantidos ao abrigo da CEDH ([12]). Além disso, o direito primário e o direito derivado têm de ser interpretados e aplicados de modo compatível com os referidos direitos ([13]). Se considerar que os seus direitos, incluindo os direitos à privacidade e à proteção dos dados, foram violados por autoridades públicas, qualquer pessoa singular pode obter reparação junto dos tribunais do Reino Unido ao abrigo do *Human Rights Act 1998* e, em última instância, depois de esgotar todos os recursos a nível nacional, pode obter reparação junto do Tribunal Europeu dos Direitos Humanos por violações dos direitos garantidos ao abrigo da CEDH.

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

(11) O Reino Unido saiu da União 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 jurídico em matéria de proteção de dados pessoais no Reino Unido que rege o tratamento de dados pessoais efetuado pelas autoridades competentes para efeitos de prevenção, investigação, deteção e repressão de infrações penais ou da execução de sanções penais, incluindo a salvaguarda e a prevenção das ameaças à segurança pública, consistia nas partes pertinentes do *Data Protection Act 2018*, que transpôs a Diretiva (UE) 2016/680.

(12) Para preparar a saída da UE, o Governo do Reino Unido promulgou o *European Union (Withdrawal) Act 2018* [Lei de 2018 sobre (a Retirada da) União Europeia] (EUWA) ([15]), que incorporava legislação da União diretamente aplicável no direito do Reino Unido e previa que a denominada «legislação interna derivada da UE» continuaria a ter efeito após o fim do período de transição. A parte 3 do DPA 2018 ([16]) que transpôs a Diretiva (UE) 2016/680 constitui «legislação interna derivada da UE» ao abrigo do EUWA. De acordo com o EUWA, a «legislação interna derivada da UE» tem de ser interpretada pelos tribunais do Reino Unido em conformidade com a jurisprudência pertinente do Tribunal de Justiça da União Europeia (Tribunal de Justiça) e os princípios gerais do direito da União em vigor imediatamente antes do fim do período de transição (designados por «jurisprudência da UE mantida» e «princípios gerais do direito da UE mantidos», respetivamente) ([17]).

(13) Ao abrigo do EUWA, os ministros do Reino Unido têm o poder de introduzir atos de direito derivado, através de instrumentos estatutários, para proceder às alterações necessárias ao direito da UE mantido em consequência da saída do Reino Unido da União Europeia. Os *Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019* [Regulamentos de 2019 relativos à Proteção dos Dados, à Privacidade e às Comunicações Eletrónicas (alterações, etc.) (saída da UE) — Regulamentos DPPEC] ([18]) exercem este poder. Os referidos regulamentos alteram a legislação em matéria de proteção de dados do Reino Unido, incluindo o DPA 2018, por motivos de compatibilidade com o contexto interno ([19]).

([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) («Acordo de Saída» ou «WA»), disponível na seguinte ligação: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:12019W/TXT(02)&from=PT

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

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

([17]) *Section 6* do EUWA 2018.

([18]) *Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019*, disponíveis na seguinte ligação: https://www.legislation.gov.uk/uksi/2019/419/contents/made, com a redação que lhe foi dada pelo DPPEC 2020, disponível na seguinte ligação: https://www.legislation.gov.uk/ukdsi/2020/9780348213522

([19]) O regulamento sobre a saída efetua um conjunto de alterações à parte 3 do DPA 2018. Muitas delas são alterações técnicas, como a supressão de referências ao «Estado-Membro» ou à «Diretiva Proteção de Dados na Aplicação da Lei» [ver, por exemplo, *section 48(8)* ou *section 73(5)(a)* do DPA 2018], substituindo-as por «direito interno», para que a parte 3 funcione efetivamente como direito interno após o fim do período de transição. Nalgumas partes, foi necessário outro tipo de alterações, por exemplo, no que respeita a «quem» adota «decisões de adequação» para efeitos do quadro jurídico do Reino Unido em matéria de proteção de dados (ver *section 74A* do DPA 2018), ou seja, o ministro da tutela em vez da Comissão Europeia.

(14) Por conseguinte, as normas jurídicas sobre o tratamento de dados pessoais efetuado pelas autoridades competentes para efeitos de prevenção, investigação, deteção e repressão de infrações penais ou da execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública no Reino Unido após o período de transição ao abrigo do Acordo de Saída continuarão a ser estabelecidas nas partes pertinentes do DPA 2018, mas com a redação que lhe foi dada pelos Regulamentos DPPEC, em particular na parte 3 da referida lei. O Regulamento Geral sobre a Proteção de Dados do Reino Unido (RGPD do Reino Unido) não é aplicável a este tipo de tratamento.

(15) A parte 3 do DPA 2018 prevê as regras de tratamento de dados pessoais para fins de aplicação do direito penal, incluindo princípios em matéria de proteção de dados, fundamentação jurídica para o tratamento (licitude), direitos dos titulares dos dados, obrigações das autoridades competentes enquanto responsáveis pelo tratamento e restrições relativas a transferências ulteriores. Ao mesmo tempo, são previstas regras em matéria de supervisão, cumprimento e recurso aplicáveis ao setor da aplicação da lei nas partes 5 e 6 do DPA 2018.

(16) Além disso, à luz do papel relevante desempenhado pelas forças policiais no setor da aplicação da lei, há que ter em consideração as regras que regem a ação da polícia. Uma vez que a ação da polícia é uma matéria delegada, são aplicáveis diversos atos legislativos, que, porém, são muitas vezes semelhantes no que respeita ao seu conteúdo, à ação da polícia a) na Inglaterra e no País de Gales, b) na Escócia e c) na Irlanda do Norte ([20]). Além disso, diversos tipos de documentos de orientação proporcionam clarificações adicionais sobre a melhor forma de utilizar os poderes da polícia. Existem três tipos principais de orientações policiais: 1) orientações legais emitidas ao abrigo de legislação, como o *Code of Ethics* (código deontológico) ([21]) e o *Code of Practice on the Management of Police Information* (código de boas de práticas para a gestão da informação da polícia – código de boas práticas MoPI) ([22]) emitido ao abrigo do *Police Act 1996* (Lei de 1996 relativa à Polícia) ([23]) ou os códigos PACE ([24]) publicados ao abrigo do *Police and Criminal Evidence Act* (Lei relativa à Polícia e aos e Meios de Prova Penal) ([25]), 2) a *Authorised Professional Practice on the Management of Police Information* (prática profissional autorizada para a gestão da informação Policial) ([26]) (orientações de PPA para a gestão da informação policial), emitida pelo *College of Policing* (Academia de Polícia), e 3) orientações operacionais (publicadas pela própria polícia). O *National Police Chiefs' Council* (Conselho Nacional de Chefias Policiais) (um organismo coordenador para todas as forças policiais do Reino Unido) publica orientações operacionais, aprovadas por todas as forças policiais e, por conseguinte, aplicáveis a nível nacional ([27]). Estas orientações têm como objetivo assegurar a coerência entre as forças no que respeita às formas de gestão da informação ([28]).

(17) O código de boas práticas MoPI foi emitido pelo ministro da tutela (*Secretary of State*) em 2005, por meio dos poderes previstos na *section 39A* do *Police Act 1996* ([29]). Qualquer código de boas práticas publicado ao abrigo do *Police Act* tem de ser aprovado pelo ministro da tutela e é objeto de consulta à *National Crime Agency* antes de ser apresentado ao parlamento. A *section 39A(7)* do *Police Act* exige que a polícia tenha devidamente em conta os códigos emitidos

([20]) Para uma explicação mais pormenorizada sobre as forças policiais e os respetivos poderes no Reino Unido, ver: *UK Explanatory Framework for Adequacy Discussions, Section F: Law Enforcement* (ver nota de rodapé 9).

([21]) *Code of Practice for the Principles and Standards of Professional Behaviour for the Policing Profession of England and Wales* (código de boas práticas para os princípios e as normas de comportamento profissional da profissão policial na Inglaterra e no País de Gales), disponível na seguinte ligação: https://www.college.police.uk/What-we-do/Ethics/Documents/Code_of_Ethics.pdf; *Police Service Northern Ireland Code of Ethic* (código deontológico dos serviços policiais da Irlanda do Norte), disponível na seguinte ligação: https://www.nipolicingboard.org.uk/psni-code-ethics; *Code of Ethic for policing in Scotland* (código deontológico da polícia na Escócia), disponível na seguinte ligação: https://www.scotland.police.uk/about-us/code-of-ethics-for-policing-in-scotland/

([22]) *Code of Practice on the Management of Police Information*, disponível na seguinte ligação: http://library.college.police.uk/docs/APPref/Management-of-Police-Information.pdf

([23]) *Police Act 1996*, disponível na seguinte ligação: https://www.legislation.gov.uk/ukpga/1996/16/contents

([24]) Códigos de boas práticas do *Police and Criminal Evidence Act 1984* (PACE), disponíveis na seguinte ligação: https://www.gov.uk/guidance/police-and-criminal-evidence-act-1984-pace-codes-of-practice.

([25]) *Police and Criminal Evidence Act 1984*, disponível na seguinte ligação: https://www.legislation.gov.uk/ukpga/1984/60/contents

([26]) *Code of Practice on the Management of Police Information*, disponível na seguinte ligação: https://www.app.college.police.uk/app-content/information-management/management-of-police-information/

([27]) *Data Protection Manual for Police Data Protection Professionals* (manual de proteção de dados para os profissionais de proteção dos dados policiais), disponível na seguinte ligação: https://www.npcc.police.uk/2019%20FOI/IMORCC/225%2019%20NPCC%20DP%20Manual%20Draft%200.11%20Mar%202019.pdf

([28]) Por exemplo, o código de boas práticas MoPI (ver nota de rodapé 22) aplica-se à retenção de informações policiais operacionais [ver considerando 47 da presente decisão].

([29]) De acordo com as informações prestadas pelas autoridades do Reino Unido, durante o período de conversações sobre a adequação, o *College of Policing* encontrava-se a elaborar um projeto de código de prática para a gestão da informação e dos registos para substituir o código de boas práticas MoPI. The draft code was published for public consultation on 25 January 2021 and is available at following link: https://www.college.police.uk/article/information-records-management-consultation

ao abrigo da referida lei, pelo que se espera que a polícia os cumpra ([30]). Além disso, as orientações não previstas por lei (como as orientações de PPA para a gestão da informação policial) têm de ser sempre coerentes com o código de boas práticas MoPI, que prevalece sobre elas ([31]). Em todo o caso, embora possa haver determinadas situações operacionais que os obrigam a divergir destas orientações, os agentes de segurança continuam a ter de cumprir os requisitos da parte 3 do DPA 2018 ([32]).

(18) O Gabinete do Comissário para a Informação («comissário para a informação» ou «ICO») ([33]) (para mais informações sobre o ICO, ver os considerandos 93 a 109) proporciona mais orientações sobre a legislação em matéria de proteção de dados do Reino Unido relativa ao tratamento no setor da aplicação da lei. Embora não sejam juridicamente vinculativas, numa ação, os tribunais teriam de ter em consideração qualquer violação das orientações, uma vez que têm peso interpretativo e demonstram a forma como o comissário interpreta e aplica a legislação em matéria de proteção de dados ([34]).

(19) Por fim, tal como mencionado nos considerandos 8 a 10, as agências de aplicação da lei do Reino Unido têm de assegurar o cumprimento da (CEDH) e da Convenção 108.

(20) Por conseguinte, na sua estrutura e componentes principais, o quadro jurídico que rege o tratamento de dados pelas autoridades de aplicação do direito penal do Reino Unido é muito semelhante ao aplicável na UE. Tal inclui o facto de tal quadro depender não só de obrigações estabelecidas no direito interno, que foram moldadas pelo direito da UE, mas também de obrigações consagradas no direito internacional, em particular por meio da adesão do Reino Unido à CEDH e à Convenção 108, bem como por meio da 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**

(21) O âmbito material da parte 3 do DPA 2018 coincide com o âmbito de aplicação da Diretiva 2016/680, conforme especificado no seu artigo 2.º, n.º 2. A parte 3 aplica-se ao tratamento de dados pessoais por uma autoridade competente por meios total ou parcialmente automatizados, bem como ao tratamento por uma entidade competente por meios não automatizados de dados pessoais contidos num ficheiro ou a ele destinados.

(22) Além disso, para que seja abrangido pelo âmbito de aplicação da parte 3, o responsável pelo tratamento tem de ser uma «autoridade competente» e o tratamento tem de ser efetuado «para efeitos de aplicação da lei». Por conseguinte, o regime de proteção de dados avaliado na presente decisão é aplicável a todas as atividades de aplicação da lei destas autoridades competentes.

(23) 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. 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,

([30]) No processo R./the Commission of Police of the Metropolis [2014] EWCA Civ 585, o estatuto legal do código de boas práticas MoPI foi confirmado, tendo o Lorde de Recurso Ordinário (*Lord Justice*) John Laws declarado que o Comissário da Polícia Metropolitana estava obrigado a ter em conta o código de boas práticas MoPI e as orientações de PPA para a gestão da informação policial em conformidade com a *section 39A* do *Police Act 1996*.

([31]) A polícia é inspecionada quanto ao cumprimento do código de boas práticas MoPI por parte do (Inspeção Real dos Serviços Policiais e de Bombeiros e Salvamento) (HMICFRS).

([32]) Ver, a este respeito, a posição do *College of Policing* sobre o cumprimento das orientações de PPA em todos os elementos do policiamento, que explica que a «PPA é autorizada pelo organismo profissional para a polícia (o *College of Policing*) enquanto fonte oficial da prática profissional em matéria de policiamento. Espera-se que os agentes de segurança e pessoal policial tenham em conta a PPA no exercício das suas responsabilidades. No entanto, podem surgir circunstâncias em que existem motivos operacionais legítimos para que a força policial divirja das orientações de PPA, contanto que haja uma lógica clara para tal. Por conseguinte, caberia à força policial assumir a responsabilidade por qualquer risco local e nacional decorrente de um funcionamento que não se enquadra nas orientações acordadas a nível nacional, sendo a força policial responsável por qualquer risco se, consequentemente, ocorrer um incidente ou for efetuada uma investigação», disponível na seguinte ligação https://www.app.college.police.uk/faq-page/

([33]) *Guide to Law Enforcement Processing* (guia para o tratamento de dados na aplicação da lei), disponível na seguinte ligação: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/

([34]) Ver processo Bridges/the Chief Constable of South Wales Police [2019] EWHC 2341 (Admin) em que, embora tome nota da natureza não vinculativa das orientações do comissário, o *High Court* (Tribunal Superior) afirmou que «[a]o considerar se um responsável pelo tratamento de dados cumpriu a obrigação constante da *section 64* [realizar uma avaliação de impacto sobre a proteção de dados em relação ao tratamento de elevado risco], os tribunais terão em conta as orientações publicadas pelo comissário para a informação no que respeita às avaliações de impacto sobre a proteção de dados».

o Comissário para o *Her Majesty's Revenue and Customs* (serviço real de fiscalidade e alfândegas do Reino Unido), 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 ([35]). A parte 3 do DPA 2018 aplica-se igualmente aos tribunais sempre que estes exercem a suas funções jurisdicionais, exceto a parte relacionada com os direitos dos titulares dos dados e a supervisão do ICO ([36]). A lista de autoridades competentes prevista no *schedule 7* não é definitiva, podendo ser atualizada pelo ministro da tutela por meio de regulamentação, tendo em conta as alterações na organização das funções públicas ([37]).

(24) O tratamento em causa tem igualmente de ser realizado «para efeitos de aplicação da lei», expressão pela qual se entende a prevenção, a investigação, a deteção ou a repressão de infrações penais ou a execução de sanções penais, incluindo a salvaguarda da segurança pública e a prevenção de ameaças à segurança pública ([38]). O tratamento por uma autoridade competente não se rege pela parte 3 do DPA 2018 se não for realizado para efeitos de aplicação da lei. É esse o caso, por exemplo, quando a *Competition and Markets Authority* investiga casos que não são tipificados como infrações penais (por exemplo, fusões entre empresas). Neste caso, será aplicável o RGPD do Reino Unido, lido em conjugação com a parte 2 do DPA 2018, uma vez que o tratamento por autoridades competentes é efetuado para fins diversos da aplicação da lei. Para determinar que regime de proteção de dados é aplicável (parte 3 ou parte 2 do DPA 2018) no tratamento dos dados pessoais em causa, a autoridade competente, ou seja, o responsável pelo tratamento, tem de apurar se a «finalidade principal» do tratamento é uma das finalidades de aplicação da lei abrangidas pelo DPA 2018.

(25) Quanto ao âmbito territorial da parte 3 do DPA 2018, a *section 207(2)*, determina que o DPA se aplica ao tratamento de dados pessoais no contexto das atividades de pessoas estabelecidas em todo o território do Reino Unido. Tal inclui autoridades públicas dos territórios da Inglaterra, do País de Gales, da Escócia e da Irlanda do Norte abrangidas pelo âmbito material da parte 3 do DPA 2018 ([39]).

2.3.1. *Definição de dados pessoais e tratamento*

(26) Os conceitos importantes de «dados pessoais» e «tratamento» são definidos na *section 3* do DPA 2018 e aplicam-se a todo o DPA. As definições seguem rigorosamente as definições correspondentes constantes do artigo 3.º da Diretiva (UE) 2016/680. No âmbito do DPA 2018, por «dados pessoais» entende-se quaisquer informações relativas a uma pessoa viva identificada ou identificável ([40]). Nos termos da *section 3(3)* do DPA 2018, é considerada identificável uma pessoa que possa ser identificada, direta ou indiretamente, a partir das informações, incluindo por referência a um nome ou um identificador ou por referência a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social. Por «tratamento» entende-se uma operação ou um conjunto de operações efetuadas sobre informações, ou conjuntos de informações, nomeadamente a) a recolha, o registo, a organização, a estruturação ou a conservação; b) a adaptação ou alteração; c) a recuperação, a consulta ou a utilização; d) a divulgação por transmissão, difusão ou por qualquer outra forma de disponibilização; e) a comparação ou interconexão; ou f) a limitação, o apagamento ou a destruição. Além disso, a lei define «tratamento sensível» como «a) o tratamento de dados pessoais que revelam a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas ou a filiação sindical; b) o tratamento de dados genéticos, ou de dados biométricos, para destinados a identificar uma pessoa de forma inequívoca; c) o tratamento de dados relativos à saúde; d) o tratamento de dados relativos à vida sexual ou à orientação sexual» ([41]). A este respeito, a *section 205* do DPA 2018 fixa as definições de «dados biométricos» ([42]), «dados relativos à saúde» ([43]) e «dados genéticos» ([44]).

([35]) Nomeadamente, 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.

([36]) *Section 43(3)* do DPA 2018.

([37]) *Section 30(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 [ver *section 30(2)* do DPA 2018], não se aplicando a parte 3 do DPA 2018 a nenhuma das suas atividades. As suas atividades são abrangidas pelo âmbito de aplicação da parte 4 do DPA 2018.

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

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

([40]) Os dados pessoais relativos a pessoas falecidas não são abrangidos pelo âmbito de aplicação do DPA 2018.

([41]) *Section 35(8)* do DPA 2018.

([42]) Por «dados biométricos» entende-se os dados pessoais resultantes de um tratamento técnico específico relativo às características físicas, fisiológicas ou comportamentais de uma pessoa que permitem ou confirmam a identificação única dessa pessoa, nomeadamente imagens faciais ou dados dactiloscópicos.

([43]) Por «dados relativos à saúde» entende-se os dados pessoais relacionados com a saúde física ou mental de uma pessoa, incluindo a prestação de serviços de saúde, que revelem informações sobre o seu estado de saúde.

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

(27) A *section 32* do DPA 2018 clarifica as definições de «responsável pelo tratamento» e «subcontratante» no contexto do tratamento de dados pessoais para efeitos de aplicação da lei seguindo rigorosamente as definições equivalentes da Diretiva (UE) 2016/680. Por «responsável pelo tratamento» entende-se a autoridade competente, que determina as finalidades e os meios do tratamento de dados pessoais. Se o tratamento for exigido por lei, o responsável pelo tratamento é a autoridade competente a que incumbe tal obrigação imposta pela lei em causa. Por «subcontratante» entende-se qualquer pessoa que proceda ao tratamento de dados pessoais em nome do responsável pelo tratamento (que não uma pessoa que seja um funcionário do responsável pelo tratamento).

2.4. **Garantias, direitos e obrigações**

2.4.1. *Licitude e lealdade do tratamento*

(28) Em conformidade com a *section 35* do DPA 2018, os dados pessoais têm de ser objeto de um tratamento lícito e leal, à semelhança do artigo 4.º, n.º 1, alínea a), da Diretiva (UE) 2016/680. Em conformidade com a *section 35(2)* 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 ou o tratamento for necessário ao exercício de funções de uma autoridade competente para essa finalidade.

2.4.1.1. Tratamento previsto na lei

(29) À semelhança do artigo 8.º da Diretiva (UE) 2016/680, para garantir a licitude de um tratamento abrangido pela parte 3 do DPA 2018, este tratamento tem de «estar previsto na lei». Por tratamento «lícito» entende-se o tratamento autorizado por lei, jurisprudência ou prerrogativa real ([45]).

(30) Os poderes das autoridades competentes regem-se, de modo geral, por leis, o que significa que as suas funções e poderes são estabelecidos de modo claro na legislação adotada pelo parlamento ([46]). Em determinados casos, a polícia e outras autoridades competentes constantes do *schedule 7* do DPA 2018 podem contar com a jurisprudência para proceder ao tratamento de dados ([47]). A jurisprudência tem-se desenvolvido por meio de precedentes estabelecidos por decisões dos tribunais. A jurisprudência é pertinente no contexto dos poderes conferidos à polícia, que deriva desta fonte de lei o seu dever essencial de proteger o público mediante a deteção e prevenção da criminalidade ([48]). Porém, as forças policiais

([45]) Notas explicativas do DPA 2018, n.º 181, disponível no seguinte endereço: https://www.legislation.gov.uk/ukpga/2018/12/pdfs/ /ukpgaen_20180012_en.pdf

([46]) A *National Crime Agency*, por exemplo, deriva os seus poderes do *Crime and Courts Act 2013* (Lei de 2013 relativa à Criminalidade e aos Tribunais), disponível na seguinte ligação https://www.legislation.gov.uk/ukpga/2013/22/contents. De modo semelhante, os poderes da *Food Standards Agency* (Agência para as Normas Alimentares) estão previstos no *Food Standards Act 1999* (Lei de 1999 relativa às Normas Alimentares), disponível na seguinte ligação https://www.legislation.gov.uk/ukpga/1999/28/contents. A título de exemplo, pode-se referir o *Prosecution of Offenders Act 1985* (Lei de 1985 relativa ao Exercício da Ação Penal contra Infratores), que criou o *Crown Prosecution Service* (Ministério Público) (ver https://www.legislation.gov.uk/ukpga/1985/23/contents); o *Commissioners for Revenue and Customs Act 2005* (Lei de 2005 relativa aos Comissários para a Fiscalidade e as Alfândegas), que estabelece o *Her Majesty's Revenue and Customs* (ver https://www.legislation.gov.uk/ukpga/2005/11/contents); o *Criminal Procedure (Scotland) Act 1995* [Lei de 1995 (da Escócia) relativa ao Processo Penal], que criou a *Scottish Criminal Cases Review Commission* (Comissão Escocesa para a Investigação de Infrações Penais) (ver https://www.legislation.gov.uk/ukpga/1995/46/contents); o *Justice (Northern Ireland) Act 2002* [Lei de 2002 (da Irlanda do Norte) relativa à Justiça], que criou o *Public Prosecution Service* (Ministério Público) na Irlanda do Norte (ver https://www.legislation.gov.uk/ukpga/2002/26/contents) e o *Serious Fraud Office* (Serviço para as Fraudes Graves) foi criado pelo *Criminal Justice Act 1987* (Lei de 1987 relativa à Justiça Penal), que lhe conferiu os poderes (ver https://www.legislation.gov.uk/ukpga/ /1987/38/contents).

([47]) Por exemplo, de acordo com as informações prestadas pelas autoridades do Reino Unido, no *Crown Office and Procurator Fiscal Service* (Ministério Público), responsável pela ação penal em processos na Escócia, o Procurador-Geral (*Lord Advocate*), que é o dirigente do sistema de ação penal na Escócia, deriva da jurisprudência os seus poderes de investigação de mortes e exercício da ação penal, ao passo que algumas das suas funções são estabelecidas por lei. Além disso, a Coroa e, por extensão, diversos governos, departamentos e ministros também derivam os seus poderes de uma combinação de legislação, jurisprudência e prerrogativa real (poderes consuetudinários conferidos à Coroa, mas exercidos por ministros).

([48]) *UK Explanatory Framework for Adequacy Discussions, Section F: Law Enforcement*, p. 8 (ver nota de rodapé 9).

dispõem de poderes decorrentes tanto da jurisprudência como da legislação ([49]) para cumprir esse dever. Sempre que a polícia tenha poderes estatutários, estes prevalecem sobre os poderes decorrentes da jurisprudência ([50]).

(31) Os tribunais têm reconhecido que o alcance dos poderes e das obrigações dos agentes de segurança decorrentes da jurisprudência abrange «todas as medidas que se afiguram necessárias para manter a paz, prevenir a criminalidade ou para proteger a propriedade contra infrações penais» ([51]). Os poderes decorrentes da jurisprudência não são absolutos. Estão sujeitos a um conjunto de limitações, incluindo limites estabelecidos pelos tribunais ([52]) e pela legislação, em particular o *Human Rights Act 1998* e o *Equality Act 2010* (Lei de 2010 relativa à Igualdade) ([53]). Além disso, para o tratamento de dados pelas autoridades competentes ao abrigo da parte 3 do DPA 2018, tal implica que o exercício dos poderes decorrentes da jurisprudência seja coerente com os requisitos estabelecidos no DPA 2018 ([54]). Acresce que as decisões para realizar qualquer tipo de tratamento de dados têm de ter em conta os requisitos das orientações aplicáveis, como o código de boas práticas MoPI, bem como as orientações específicas de um dos países do Reino Unido ([55]). O governo e os organismos operacionais da polícia emitem diversos documentos de orientação para assegurar que os agentes de segurança exercem os seus poderes de tratamento dentro dos limites fixados pela jurisprudência e pela legislação pertinente ([56]).

(32) As prerrogativas reais constituem uma outra componente da «lei» e dizem respeito a determinados poderes investidos na Coroa suscetíveis de serem exercidos pelo executivo e que não se baseiam na legislação, mas derivam da soberania do monarca ([57]). Existem muito poucos exemplos de poderes de prerrogativa pertinentes no contexto da aplicação da lei. Entre eles, inclui-se, por exemplo, o quadro de auxílio judiciário mútuo que permite a partilha

([49]) Os principais atos legislativos que estabelecem o regime dos principais poderes policiais (detenção, busca, autorização da prorrogação da detenção, recolha de impressões digitais, recolha de amostras íntimas, interceção por mandado, acesso a dados de comunicação) são: i) para a Inglaterra e o País de Gales, o *Police and Criminal Evidence Act 1984* (PACE), disponível na seguinte ligação: https://www.legislation.gov.uk/ukpga/1984/60/contents (com a redação que lhe foi dada pelo *Protection of Freedoms Act 2012* (Lei de 2012 relativa à Proteção das Liberdades) (PoFA), disponível na seguinte ligação: https://www.legislation.gov.uk/ukpga/2012/9/contents) e o *Investigatory Powers Act 2016* (Lei de 2016 relativa aos Poderes de Investigação) (IPA), disponível na seguinte ligação: https://www.legislation.gov.uk/ukpga/2016/25/contents), ii) para a Escócia, o *Criminal Justice (Scotland) Act 2016* [Lei de 2016 (da Escócia) relativa à Justiça Penal], disponível na seguinte ligação: https://www.legislation.gov.uk/asp/2016/1/contents e o *Criminal Procedure (Scotland) Act 1995*, disponível na seguinte ligação: https://www.legislation.gov.uk/ukpga/1995/46/contents), iii) para a Irlanda do Norte, o *Police and Criminal Evidence (Northern Ireland) Order 1989* [Decreto de 1989 (da Irlanda do Norte) relativo à polícia e aos meios de prova penal], disponível na seguinte ligação: https://www.legislation.gov.uk/nisi/1989/1341/contents

([50]) As autoridades do Reino Unido explicaram que o princípio da supremacia das disposições legislativas já se encontra há muito estabelecido no Reino Unido, remontando ao acórdão proferido no processo Entick/Carrington [1765] EWHC KB J98, que reconheceu que existem limites ao exercício dos poderes do executivo e estabeleceu o princípio da subordinação dos poderes decorrentes da jurisprudência e de prerrogativa do monarca e do governo à legislação do país.

([51]) Ver processo Rice/Connolly [1966] 2 QB 414.

([52]) Ver processo R(Catt)/Association of Chief police Officers [2015] AC 1065, em que, no que respeita ao poder policial para obter e conservar informações de uma pessoa singular (que cometeu uma infração penal), Lorde Jonathan Sumption considerou que, ao abrigo da jurisprudência, a polícia tem o poder de obter e conservar informação para fins policiais, ou seja, em termos gerais, para a manutenção da ordem pública e a prevenção e deteção da criminalidade. Estes poderes não permitem métodos intrusivos de obtenção de informação, como a entrada em propriedade privada ou atos (que não a detenção ao abrigo dos poderes decorrentes da jurisprudência) que constituam uma agressão. O juiz considerou que, neste caso, os poderes decorrentes da jurisprudência eram suficientes para permitir a obtenção e a conservação do tipo de informação pública em causa nestes recursos.

([53]) *Equality Act 2010*, disponível na seguinte ligação: https://www.legislation.gov.uk/ukpga/2010/15/contents

([54]) Para um exemplo de um processo em que os poderes da polícia decorrentes da jurisprudência são analisados no quadro do DPA 1998, ver a decisão do *High Court* no processo Bridges/the Chief Constable of South Wales Police (ver nota de rodapé 33). Ver, igualmente, os processos *Vidal-Hall/Google Inc.* [2015] EWCA Civ 311 e *Richard/BBC* [2018] EWHC 1837 (Ch).

([55]) Ver, por exemplo, a orientação do *Police Service of Northern Ireland* constante das instruções de serviço sobre a gestão de registos, disponível na seguinte ligação: https://www.psni.police.uk/globalassets/advice–information/our-publications/policies-and-service--procedures/records-management-080819.pdf

([56]) A Câmara dos Comuns publicou um documento informativo que explica os principais poderes policiais decorrentes da jurisprudência e da legislação na Inglaterra e no País de Gales (ver https://researchbriefings.files.uk/documents/CBP-8637/CBP-8637.pdf). De acordo com este documento, por exemplo, não obstante o facto de os poderes de manutenção «da paz do Reino» derivarem da jurisprudência, bem como «o uso da força», «os poderes para parar e revistar» derivam sempre da legislação. Além disso, o Governo escocês proporciona informações no seu sítio Web sobre os poderes policiais de detenção e para parar e revistar (ver https://www.gov.scot/policies/police/police-powers/).

([57]) De acordo com a informação prestada pelas autoridades do Reino Unido, os poderes de prerrogativa exercidos pelo governo incluem, por exemplo, a celebração e ratificação de tratados, a diplomacia, o uso das forças armadas no Reino Unido para manter a paz em apoio da polícia.

de dados por um ministro com países terceiros para efeitos de aplicação da lei, não estando sempre estatuído o poder de partilhar dados deste modo ([58]). As prerrogativas reais estão sujeitas a princípios da jurisprudência ([59]) e subordinam-se à legislação, estando, por conseguinte, sujeitas aos limites previstos no *Human Rights Act 1998* e no DPA 2018 ([60]).

(33) À semelhança do artigo 8.º da Diretiva (UE) 2016/680, o regime do Reino Unido exige que, para cumprir o princípio da licitude, as autoridades competentes assegurem que, quando se baseia na lei, o tratamento seja «necessário» para levar a cabo a incumbência para uma finalidade de aplicação da lei. O ICO proporciona uma orientação a este respeito, esclarecendo que «tem de constituir uma forma específica e proporcionada de alcançar a finalidade. Não haverá uma base lícita se for possível alcançar a finalidade de modo razoável por outros meios menos intrusivos. Não basta alegar que o tratamento é necessário porque se decidiu realizar o procedimento de uma determinada forma. Trata-se de saber se o tratamento é necessário para a finalidade especificada» ([61]).

2.4.1.2. Tratamento com base no «consentimento» do titular dos dados

(34) Conforme referido no considerando 28, a section 35(2) do DPA 2018 prevê a possibilidade de proceder ao tratamento de dados pessoais com base no «consentimento» da pessoa.

(35) No entanto, o consentimento não se afigura uma base jurídica pertinente para as operações de tratamento abrangidas pelo âmbito de aplicação da presente decisão. Efetivamente, as operações de tratamento abrangidas pela presente decisão dirão sempre respeito a dados que tenham sido transferidos ao abrigo da Diretiva (UE) 2016/680 por uma autoridade competente de um Estado-Membro da UE para uma autoridade competente do Reino Unido. Por conseguinte, não envolverão, geralmente, o tipo de interação direta (recolha) entre uma autoridade pública e os titulares dos dados suscetível de basear-se no consentimento ao abrigo da *section 35(2)(a)* do DPA 2018.

(36) Embora a dependência do consentimento não seja, portanto, considerada pertinente para a avaliação realizada na presente decisão, por uma questão de exaustividade, afigura-se oportuno referir que, no contexto da aplicação da lei, o tratamento não se baseia exclusivamente no consentimento, dado que a autoridade competente tem de ter sempre um poder subjacente que lhe permite proceder ao tratamento dos dados ([62]). Mais especificamente, e à semelhança do permitido ao abrigo da Diretiva (UE) 2016/680 ([63]), tal significa que o consentimento serve de condição adicional para permitir a realização de determinadas operações de tratamento limitadas e específicas que não poderiam ser realizadas de outra forma, como, por exemplo, a recolha e o tratamento de uma amostra de ADN de uma pessoa que não seja suspeita. Neste caso, não se procederia ao tratamento se não fosse dado consentimento ou este tivesse sido retirado ([64]).

([58]) A este respeito, ver a avaliação do regime de transferência ulterior do Reino Unido nos considerandos (74)-(87).

([59]) Ver processo Bancoult/Secretary of State for Foreign and Commonwealth Affairs [2008] UKHL 61, em que os tribunais consideraram que o poder de prerrogativa de elaborar decretos-lei estava igualmente sujeito aos fundamentos ordinários da fiscalização jurisdicional.

([60]) Ver processo Attorney-General/De Keyser's Royal Hotel Ltd [1920] AC 508, em que o tribunal considerou que os poderes de prerrogativa não podem ser utilizados quando existem poderes legais que os substituem; processo *Laker Airways Ltd/Department of Trade* [1977] QB 643, em que o tribunal considerou que os poderes de prerrogativa não podem ser utilizados para frustrar a legislação; processo *R/Secretary of State for the Home Department, ex p. Fire Brigades Union* [1995] UKHL 3, em que o tribunal considerou que os poderes de prerrogativa não podem ser utilizados quando contrariam legislação promulgada, mesmo que a referida legislação ainda não tenha entrado em vigor; processo *R (Miller)/Secretary of State for Exiting the European Union* [2017] UKSC 5, em que o tribunal confirmou a capacidade de ajustar e abolir por lei os poderes de prerrogativa. Para uma visão geral da relação entre as prerrogativas reais e os poderes decorrentes da legislação ou da jurisprudência, ver o artigo informativo da Câmara dos Comuns, disponível na seguinte ligação: https://researchbriefings.files.parliament.uk/documents/SN03861/SN03861.pdf

([61]) *Guide to Law Enforcement Processing, «What is the first principle about?»* (guia para o tratamento de dados na aplicação da lei, «Qual o seu primeiro princípio?»), disponível na seguinte ligação: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/principles/#ib2

([62]) Tal decorre do texto da disposição pertinente do DPA 2018, segundo a qual o tratamento de dados pessoais para efeitos de aplicação da lei só é lícito se e na medida em que «estiver previsto na lei» e se a) o titular dos dados tiver dado o seu consentimento ao tratamento para essa finalidade, ou b) o tratamento for necessário ao exercício de funções de uma autoridade competente para essa finalidade.

([63]) Ver considerandos 35 e 37 do Regulamento (UE) 2016/680.

([64]) As autoridades do Reino Unido explicaram que, por exemplo, uma situação em que o consentimento pode constituir uma base adequada para proceder ao tratamento seria quando a polícia obtém uma amostra de ADN relacionada com uma pessoa desaparecida para compará-la com um corpo que eventualmente seja encontrado. Nestas circunstâncias, seria impróprio que a polícia obrigasse o titular dos dados a fornecer uma amostra. Em vez disso, a polícia solicitaria o consentimento da pessoa, que é livremente dado e pode ser retirado a qualquer momento. Se o consentimento for retirado, os dados não podem ser objeto de tratamento, a menos que se estabeleça uma nova base jurídica para continuar o tratamento da amostra (por exemplo, o titular dos dados tornou-se um suspeito). Poderia surgir uma outra situação, por exemplo, em que a força policial investiga uma infração penal em que a vítima (que pode ser a vítima de um assalto, de um delito sexual ou de violência doméstica, os parentes de uma vítima de homicídio ou outra vítima de infrações penais) beneficiaria de uma referenciação junto da Victim Support (uma organização de beneficência independente dedicada ao apoio às pessoas afetadas pela criminalidade e incidentes traumáticos). Nestas circunstâncias, a polícia apenas partilhará informações pessoais como o nome e os dados de contacto com a Victim Support se obtiverem o consentimento da vítima.

(37) Nos casos que exigem o consentimento da pessoa singular, este consentimento tem de ser explícito e implicar um ato positivo inequívoco ([65]). As forças policiais estão obrigadas a ter um aviso de privacidade que inclua, nomeadamente, a informação necessária relacionada com a utilização válida do consentimento. Além disso, algumas delas publicam materiais adicionais sobre o cumprimento da legislação em matéria de proteção de dados, incluindo como e quando recorrem ao consentimento enquanto base jurídica ([66]).

2.4.1.3. Tratamento sensível

(38) Devem existir garantias específicas aplicáveis ao tratamento de «categorias especiais» de dados. A este respeito, à semelhança do previsto no artigo 10.º da Diretiva (UE) 2016/680, a parte 3 do DPA 2018 prevê garantias mais robustas para o designado «tratamento de dados sensíveis» ([67]).

(39) Nos termos da *section 35(3)* do DPA 1998, as autoridades competentes só podem proceder ao tratamento de dados sensíveis para efeitos de aplicação da lei em dois casos: 1) se o titular dos dados tiver dado consentimento para o tratamento para efeitos de aplicação da lei e, no momento em que o tratamento é realizado, o responsável pelo tratamento dispõe de um documento de políticas adequado ([68]); ou 2) o tratamento é estritamente necessário para efeitos de aplicação da lei, cumpre pelo menos uma das condições constantes do *schedule 8* do DPA 2018 e, no momento em que o tratamento é realizado, o responsável pelo tratamento dispõe de um documento de políticas adequado ([69]).

(40) No que respeita ao primeiro caso, conforme explicado no considerando 38, a necessidade do consentimento não é considerada pertinente no tipo de situação de transferência objeto da presente decisão ([70]).

(41) Quando o tratamento de dados sensíveis não depende do consentimento, pode ser realizado nas condições prevista no *schedule 8* do DPA 2018. Estas condições estão relacionadas com o processamento necessário para fins previstos na lei; a administração da justiça; a proteção dos interesses vitais do titular de dados ou de um terceiro; a salvaguarda de crianças e pessoas em risco; os direitos em processos judiciais; os atos judiciais; a prevenção da fraude; o arquivo; se os dados pessoais tenham sido manifestamente tornados públicos pelo seu titular. Para além do caso em que os dados são manifestamente tornados públicos, todas as condições previstas no *schedule 8* estão sujeitas

([65]) Não existe uma definição independente de «consentimento» para efeitos de tratamento de dados pessoais ao abrigo da parte 3 do DPA 2018. O ICO forneceu orientações sobre a noção de «consentimento» ao abrigo da parte 3 do DPA 2018, esclarecendo que o termo tem o mesmo sentido e deve ser consentâneo com a definição prevista no RGPD, nomeadamente que «o consentimento tem de ser dado de livre vontade e tem de haver uma escolha genuína quanto à aceitação do tratamento dos dados» [*Guide to Law Enforcement Processing*, *«What is the first principle about?»* (ver nota de rodapé 64) e *Guide to Data Protection* (guia para a proteção dos dados), na parte relativa ao consentimento, disponível na seguinte ligação: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the--general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/).

([66]) Ver, por exemplo, as informações constantes da página Web da polícia de Lincolnshire (ver https://www.lincs.police.uk/resource--library/data-protection/law-enforcement-processing/) ou na página Web da polícia de West Yorkshire (https://www.westyorkshire.police.uk/sites/default/files/2018-06/data_protection.pdf).

([67]) *Section 35(8)* do DPA 2018.

([68]) *Section 35(4)* do DPA 2018.

([69]) *Section 35(5)* do DPA 2018.

([70]) Por uma questão de exaustividade, afigura-se oportuno referir que, quando o tratamento se baseia no consentimento, este tem de ser dado de livre vontade, específico e informado e tem de haver uma escolha específica quanto à aceitação do tratamento dos dados. Além disso, o responsável pelo tratamento, ao proceder ao tratamento com base no consentimento do titular dos dados, está obrigado a ter um documento de políticas adequado (*appropriate policy document*, APD). A *section 42* do DPA 2018 descreve em termos gerais os requisitos que o APD tem de observar. Torna claro que o documento, no mínimo, tem de explicar os procedimentos do responsável pelo tratamento para assegurar o cumprimento dos princípios da proteção de dados e explicar as políticas do responsável pelo tratamento no que respeita à conservação e ao apagamento de dados pessoais. Nos termos da *section 42* do DPA 2018, tal significa que o responsável pelo tratamento tem de elaborar um documento que a) explique os procedimentos do responsável pelo tratamento para garantir o cumprimento dos princípios da proteção de dados; e b) explique as políticas do responsável pelo tratamento em matéria de conservação e apagamento de dados pessoais tratados com base no consentimento do titular dos dados ou que dê uma indicação do tempo durante o qual os referidos dados pessoais são provavelmente conservados. Mais particularmente, o documento de políticas exige que o responsável pelo tratamento, no cumprimento do seu dever de registo das atividades de tratamento, inclua sempre os elementos mencionados nas alíneas a) e b). O ICO publicou um modelo do referido documento [*Guide to Law Enforcement Processing*. *«Conditions for sensitive processing»* (guia para o tratamento de dados na aplicação da lei. «Condições para o tratamento sensível»), disponível na seguinte ligação: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law--enforcement-processing/conditions-for-sensitive-processing) e pode tomar medidas coercivas se os responsáveis pelo tratamento não cumprirem estes requisitos. O APD é também examinado pelos tribunais ao analisarem possíveis violações do DPA 2018. Por exemplo, no recente processo *R (Bridges)/Chief Constable of South Wales Police*, os tribunais analisaram o APD do responsável pelo tratamento e consideram-no adequado, mas teria sido útil se fosse mais detalhado. Por conseguinte, a polícia de Gales do Sul reviu o APD e atualizou-o em consonância com as novas orientações do ICO (ver nota de rodapé 33). Além disso, em conformidade com a *section 42(3)* do DPA 2018, o APD deve ser revisto periodicamente pelo responsável pelo tratamento. Por fim, a título de garantia adicional, em conformidade com a *section 42(4)* do DPA 2018, o responsável pelo tratamento está obrigado a manter um registo alargado das atividades de tratamento, incluindo elementos adicionais em relação à obrigação geral que incumbe ao responsável pelo tratamento no âmbito das atividades de tratamento estabelecida na *section 61* do DPA 2018.

ao teste da «estrita necessidade». Tal como esclarecido pelo ICO, «neste contexto, por «estritamente necessário» entende-se que o tratamento tem de estar relacionado com uma necessidade social premente que não pode ser alcançada razoavelmente por meios menos intrusivos» ([71]). Além disso, algumas das condições estão sujeitas a limitações adicionais. Por exemplo, para que se possa recorrer à condição relativa aos «fins previstos na lei» e à «condição relativa à salvaguarda» (*schedule 8*, n.os 1 e 4) é necessário realizar o teste adicional do interesse público importante. Além disso, no que respeita às condições relativas à salvaguarda da criança (*schedule 8*, n.º 4), é igualmente necessário que o titular dos dados também tenha uma determinada idade e que se considere que este está em risco. Além disso, o responsável pelo tratamento só pode aplicar a condição prevista no *schedule 8*, n.º 4, em circunstâncias específicas ([72]). Existem, igualmente, limitações para as condições relativas aos «atos judiciais» e à «prevenção da fraude» (*schedule 8*, n.os 7 e 8, respetivamente). Ambas só são aplicáveis a responsáveis pelo tratamento específicos. No caso dos atos judiciais, só um tribunal ou outra autoridade judicial conseguem satisfazer esta condição e, no caso da prevenção da fraude, só os responsáveis pelo tratamento que sejam organizações de luta contra a fraude conseguem satisfazer esta condição.

(42) Por fim, quando o tratamento depende de uma das condições enunciadas no schedule 8 e em conformidade com a section 42 do DPA 2018, tem de existir um «documento de políticas adequado» — que explique os procedimentos do responsável pelo tratamento para garantir o cumprimento dos princípios da proteção de dados e as políticas do responsável pelo tratamento no que respeita à conservação e ao apagamento de dados pessoais — e sendo aplicáveis as obrigações de registo alargado.

2.4.2. *Limitação das finalidades*

(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. Este princípio da proteção de dados é garantido pela *section 36* do DPA 2018. Esta disposição, à semelhança do artigo 4.º, n.º 1, alínea b), da Diretiva (UE) 2016/680, exige que a) as finalidades de aplicação da lei para que se procede à recolha de dados pessoais em qualquer momento sejam determinadas, explícitas e legítimas, e b) os dados pessoais recolhidos deste modo não sejam tratados de uma forma incompatível com a finalidade para que foram recolhidos.

(44) Quando as autoridades competentes tratam dados para efeitos de aplicação da lei, estes podem incluir fins de arquivo, fins de investigação científica ou história e fins estatísticos ([73]). Nesses casos, o DPA 2018 esclarece igualmente que o arquivo (ou o tratamento para fins de investigação científica ou histórica ou estatísticos) não é permitido se for realizado em relação a decisões relacionadas com um titular de dados específico ou se for suscetível de provocar importantes danos ou sofrimento emocional ao titular dos dados ([74]).

2.4.3. *Exatidão e minimização dos dados*

(45) Os dados têm de ser exatos e, se necessário, atualizados. Têm, igualmente, de ser adequados, pertinentes e não excessivos relativamente às finalidades para que são tratados. À semelhança do artigo 4.º, n.º 1, alíneas c), d) e e), da Diretiva (UE) 2016/680, estes princípios são garantidos nas *sections 37* e *38* do DPA 2018. É necessário tomar todas as medidas razoáveis para assegurar que os dados inexatos ([75]) sejam apagados ou retificados sem

([71]) *Guide to Law Enforcement Processing, «Conditions for sensitive processing»* (ver nota de rodapé 70).

([72]) O tratamento sem consentimento do titular dos dados realiza-se se: a) o titular dos dados não puder dar o consentimento para o tratamento; b) não for expectável que o responsável pelo tratamento consiga obter o consentimento do titular dos dados para o tratamento; c) o tratamento tiver de ser realizado sem o consentimento do titular dos dados porquanto a obtenção do consentimento do titular dos dados prejudicaria a prestação da proteção referida no subponto 1, alínea a).

([73]) Ver *section 41(1)* do DPA 2018.

([74]) Ver *section 41(2)* do DPA 2018.

([75]) Nos termos da *section 205* do DPA 2018 por «inexatos» entende-se os dados pessoais «incorretos ou suscetíveis de induzir em erro». As autoridades do Reino Unido explicaram que os dados relacionados com investigações penais são habitualmente incompletos, mas, independentemente desse facto, podem ser exatos.

demora ([76]), tendo em conta a finalidade de aplicação da lei para a qual são tratados ([77]) e para assegurar que os dados pessoais inexatos, incompletos ou que não estejam atualizados não sejam transmitidos ou disponibilizados para efeitos de aplicação da lei ([78]).

(46) Além disso, à semelhança do artigo 7.º da Diretiva (UE) 2016/680, o regime de proteção de dados do Reino Unido especifica que os dados pessoais baseados em factos têm de ser, na medida do possível, distinguidos dos dados pessoais baseados em apreciações pessoais ([79]). Se for caso disso e na medida do possível, tem de ser feita uma distinção entre os dados pessoais relativos a diferentes categorias de titulares de dados, como pessoas suspeitas, pessoas condenadas por uma infração penal, vítimas de uma infração penal e testemunhas ([80]).

2.4.4. *Limitação da conservação*

(47) Em conformidade com o artigo 5.º da Diretiva (UE) 2016/680, em princípio, os dados não devem ser conservados mais tempo do que o necessário para as finalidades para as quais são tratados. Nos termos da *section 39* do DPA 2018 e à semelhança do artigo 5.º da referida diretiva, é proibido conservar dados pessoais tratados para efeitos de aplicação da lei por mais tempo do que o necessário tendo em conta a finalidade para a qual são tratados. O regime jurídico do Reino Unido exige que sejam estabelecidos prazos adequados para a reavaliação periódica da necessidade de conservação de dados pessoais para efeitos de aplicação da lei. Foram estabelecidas regras adicionais para as práticas relativas à conservação de dados pessoais e os prazos aplicáveis na legislação pertinente e nas orientações que regem os poderes e o funcionamento da polícia. Por exemplo, na Inglaterra e no País de Gales, o código de boas práticas MoPI do *College of Policing* e as orientações de PPA para a gestão da informação policial proporcionam um quadro para garantir um processo de conservação, reavaliação e eliminação coerente e assente no risco para a gestão das informações de policiamento operacionais ([81]). Este quadro estabelece expectativas claras em todo o serviço quanto à melhor forma de criar, partilhar, utilizar e gerir a informação em cada força policial e agência e entre as mesmas ([82]). Espera-se que polícia cumpra o código de boas práticas MoPI, sendo o cumprimento verificado pelo *Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services* ([83]).

(48) O *Police Service of Northern Ireland* (PSNI) não é obrigado por lei a observar o código de boas práticas MoPI. No entanto, o quadro do código MoPI adotado em 2011 é completado pelo *PSNI Handbook* (manual da PSNI) ([84]), que estabelece políticas e procedimentos para a aplicação do código de boas práticas MoPI na Irlanda do Norte.

([76]) *Section 38(1)* do DPA 2018.

([77]) De acordo com o quadro explicativo do Reino Unido para as conversações em matéria de adequação, «tal assegura o reconhecimento tanto dos direitos dos titulares dos dados como das necessidades operacionais das autoridades de aplicação da lei. O ponto referido acima foi rigorosamente tido em conta durante as fases de elaboração do projeto do *Data Protection Bill*, uma vez que podem existir motivos operacionais específicos e limitados pelos quais os dados não podem ser retificados. Tal ocorrerá, mais provavelmente, se for necessário preservar os dados pessoais inexatos na sua forma inicial para fins probatórios» (ver *UK Explanatory Framework for Adequacy Discussions, Section F: Law Enforcement*, p. 21, ver nota de rodapé 9).

([78]) *Section 38(4)* do DPA 2018. Além disso, por força da *section 38(5)* do DPA 2018, é necessário verificar a qualidade dos dados pessoais antes de estes serem transmitidos ou disponibilizados, em todas as transmissões de dados pessoais, é necessário incluir as informações necessárias para que o destinatário possa aferir até que ponto os dados são exatos, completos e fiáveis, e estão atualizados, e é necessário notificar sem demora o destinatário caso se verifique, após a transmissão de dados pessoais, que os dados estavam incorretos ou a transmissão era ilícita.

([79]) *Section 38(2)* do DPA 2018.

([80]) *Section 38(3)* do DPA 2018.

([81]) Este quadro assegura a coerência na aplicação da conservação dos dados pessoais adquiridos. O período de reavaliação depende das infrações penais, que se dividem em quatro grupos: 1) determinadas questões de proteção pública; 2) outras infrações graves e violentas de natureza sexual; 3) todas as restantes infrações penais; 4) diversas. As orientações de PPA para a gestão da informação policial apresentam informações mais pormenorizadas (ver nota de rodapé 26).

([82]) De acordo com as informações fornecidas pelas autoridades do Reino Unido, as outras organizações podem seguir os princípios do código de boas práticas MoPI se o desejarem, por exemplo, o *Her Majesty's Revenue and Customs* e a *National Crime Agency* adotaram voluntariamente muitos dos princípios do código de boas práticas MoPI para assegurar a coerência na aplicação da lei. Em geral, a maioria das organizações fornece a todos os seus funcionários políticas e orientações específicas sobre a melhor forma de tratar os dados pessoais como parte da sua função e adaptadas à organização específica. Em geral, tal inclui igualmente formação obrigatória.

([83]) O código de boas práticas MoPI foi publicado recorrendo aos poderes concedidos ao abrigo do *Police Act 1996*, que permite que o *College of Policing* publique códigos de boas práticas relacionados com o funcionamento eficaz do policiamento. Qualquer código de boas práticas elaborado ao abrigo da referida lei tem de ser aprovado pelo ministro da tutela e é objeto de consulta à *National Crime Agency* antes de ser apresentado ao parlamento. A *section 39A(7)* do *Police Act 1996* exige que a polícia tenha em devida conta os códigos emitidos ao abrigo do *Police Act 1996*.

([84]) *PSNI MoPI Handbook*, capítulos 1 a 6.

(49) Na Escócia, as forças policiais dependem do *Record Retention Standard Operating Procedure* (procedimento operacional normalizado para a conservação de registos) (SOP) ([85]), que apoia a *Records Management Policy* (política de gestão de registos) da Autoridade Policial da Escócia ([86]). O SOP estabelece regras de conservação específicas para os registos detidos pela Autoridade Policial da Escócia.

(50) Para além do requisito global de reavaliação dos registos aplicável em todo o Reino Unido, existem regras localizadas mais pormenorizadas. Para dar alguns exemplos, no que respeita à Inglaterra e ao País de Gales, o *Police and Criminal Evidence Act*, com a redação que lhe foi dada pelo *Protection of Freedom Act 2012* (Lei de 2012 relativa à Proteção da Liberdade) (PoFA), prevê a conservação de impressões digitais e perfis de ADN, bem como um regime específico para as pessoas não condenadas ([87]). O PoFA criou igualmente a posição de Comissário para a Conservação e Utilização de Materiais Biométricos («comissário biométrico») ([88]). O estudo de 2017 relativo às imagens recolhidas em detenção estabelece as regras específicas para estas imagens ([89]). No que respeita à Escócia, o *Criminal Procedure (Scotland) Act 1995* prevê as regras para a obtenção e conservação de impressões digitais e amostras biológicas ([90]). Tal como no caso da Inglaterra e do País de Gales, a legislação regula a conservação de dados biométricos em diversos casos ([91]).

2.4.5. *Segurança dos dados*

(51) Os dados pessoais têm de 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, as autoridades públicas têm de tomar as medidas técnicas e organizativas adequadas para proteger os dados pessoais contra eventuais ameaças. Estas medidas têm de ser avaliadas tendo em consideração o estado atual dos conhecimentos e os custos conexos.

(52) Estes princípios estão espelhados na *section 40* do DPA 2018, de acordo com a qual, à semelhança do artigo 4.º, n.º 1, alínea f), da Diretiva (UE) 2016/680, os dados pessoais tratados para efeitos de aplicação da lei têm de ser tratados de uma forma que garanta a sua segurança adequada, recorrendo a medidas técnicas ou organizativas adequadas. Tal inclui a proteção dos dados contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou

([85]) *Record Retention Standard Operating Procedure* (SOP), disponível na seguinte ligação: https://www.scotland.police.uk/spa-media/nhobty5i/record-retention-sop.pdf

([86]) Para mais informações sobre a gestão de registos, ver as informações relacionadas com o *National Records of Scotland* (Serviço de Registos da Escócia), disponíveis na seguinte ligação: https://www.nrscotland.gov.uk/record-keeping/records-management

([87]) Os períodos de conservação variam conforme a pessoa tenha sido condenada ou não (*sections 63I* a *63KI* do PACE 1984). Por exemplo, no caso de um adulto condenado por infração suscetível de inscrição no registo, as suas impressões digitais e perfil de ADN podem ser conservados por tempo indeterminado [*section 63I(2)* do PACE 1984], ao passo que a conservação é temporalmente limitada se a pessoa condenada tiver menos de 18 anos, se se tratar de uma infração suscetível de inscrição no registo de «menor gravidade» e se a pessoa nunca tenha sido condenada (*section 63K* do PACE 1984). A conservação no caso de uma pessoa detida ou acusada, mas não condenada, está temporalmente limitada a três anos (*section 63F* do PACE 1984). O alargamento deste prazo de conservação tem de ser aprovado por uma autoridade judicial [*section 63F(7)* do PACE 1984]. No caso de pessoas detidas ou acusadas, mas não condenadas por uma infração de menor gravidade, não é possível conservar informações (*sections 63D* e *63H* do PACE 1984).

([88]) A *section 20* do PoFA 2012 cria o cargo de comissário biométrico, 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) [disponível na seguinte ligação: *Governance Code for Public Appointments* – GOV.UK (www.gov.uk)]. As condições de nomeação deixam claro que este só pode ser destituído pelo ministro da Administração Interna 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.

([89]) *Review of the Use and Retention of Custody Images* (estudo sobre a utilização e conservação de imagens recolhidas em detenção), disponível na seguinte ligação: https://www.gov.uk/government/publications/custody-images-review-of-their-use-and-retention

([90]) *Section 18* e seguintes do *Criminal Procedure (Scotland) Act 1995*.

([91]) Os períodos de conservação variam conforme a pessoa tenha sido condenada ou não [*section 18(3)* do *Criminal Procedure (Scotland) Act 1995*] ou seja menor ou não. Neste último caso, o período de conservação é de três anos a partir da condenação na audiência do menor [*section 18E(8)* do *Criminal Procedure (Scotland) Act 1995*]. Os dados de pessoas detidas, mas não condenadas, não podem ser conservados [*section 18(3)* do *Criminal Procedure (Scotland) Act 1995*], salvo em casos específicos dependendo da gravidade da infração penal [*section 18A* do *Criminal Procedure (Scotland) Act 1995*]. O *Scottish Biometrics Commissioner Act 2020* (Lei de 2020 relativa ao Comissário Biométrico da Escócia) (ver https://www.legislation.gov.uk/asp/2020/8/contents) cria o cargo de comissário biométrico da Escócia, que tem de elaborar e rever os códigos de boas práticas (aprovados pelo parlamento escocês) no que respeita à aquisição, à conservação, à utilização e à destruição de dados biométricos para fins de justiça penal e policiais (*section 7* do *Scottish Biometrics Commissioner Act 2020*).

danificação acidentais ([92]). A *section 66* do DPA 2018 especifica adicionalmente que cada responsável pelo tratamento e cada subcontratante tem de tomar as medidas técnicas e organizativas adequadas para assegurar um nível de segurança adequado aos riscos decorrentes do tratamento de dados pessoais. De acordo com as notas explicativas, o responsável pelo tratamento tem de avaliar os riscos e adotar as medidas de segurança adequadas com base nesta avaliação, como, por exemplo, a cifragem ou níveis específicos de credenciação de segurança do pessoal que trata os dados ([93]). A avaliação tem igualmente de ter em conta, por exemplo, a natureza dos dados tratados e quaisquer outros fatores ou circunstâncias pertinentes suscetíveis de afetarem a segurança do tratamento.

(53) O regime que rege o cumprimento dos princípios de segurança dos dados é muito semelhante ao estabelecido pelos artigos 29.º a 31.º da Diretiva (UE) 2016/680. Mais particularmente, nos termos da *section 67(1)* do DPA 2018, em caso de violação de dados pessoais da responsabilidade do responsável pelo tratamento, este último tem de notificar desse facto o comissário para a informação sem demora injustificada e, sempre que possível, até 72 horas após ter tido conhecimento da violação ([94]). A obrigação de notificar não é aplicável quando a violação dos dados pessoais não for suscetível de resultar num risco para os direitos e as liberdades das pessoas singulares ([95]). O responsável pelo tratamento tem de documentar os factos relacionados com quaisquer violações dos dados pessoais, os seus efeitos e as medidas corretivas tomadas de modo que permita ao comissário para a informação verificar a conformidade com o DPA ([96]). Se tomarem conhecimento de uma violação da segurança, os subcontratantes têm de notificar o responsável pelo tratamento sem demora injustificada ([97]).

(54) Nos termos da *section 68(1)* do DPA 2018, se uma violação dos dados pessoais for suscetível de resultar num elevado risco para os direitos e liberdades das pessoas, o responsável pelo tratamento tem de comunicar a violação de dados pessoais ao titular dos dados sem demora injustificada ([98]). Esta notificação tem de incluir as mesmas informações que a notificação ao comissário para a informação descrita no considerando 53. Esta obrigação não é aplicável se o responsável pelo tratamento tiver tomado as medidas técnicas e organizativas de proteção adequadas, que foram aplicadas aos dados pessoais afetados pela violação. Também não é aplicável se o responsável pelo tratamento tiver tomado medidas subsequentes que asseguram que o elevado risco para os direitos e as liberdades dos titulares dos dados já não é suscetível de se concretizar. Por fim, o responsável pelo tratamento não tem de notificar o titular dos dados se tal implicar um esforço desproporcionado ([99]). Nesse caso, as informações têm de ser disponibilizadas ao titular dos dados por outro modo igualmente eficaz, por exemplo, por meio de uma comunicação pública ([100]). Se o responsável pelo tratamento não tiver informado o titular dos dados da violação dos dados pessoais, o comissário para a informação, tendo sido notificado em conformidade com a *section 67* do DPA e tendo considerado a probabilidade de a violação resultar num elevado risco, pode exigir que o referido responsável pelo tratamento proceda à notificação da violação ao titular dos dados ([101]).

([92]) De acordo com as notas explicativas do DPA 2018 (ver nota de rodapé 45), o responsável pelo tratamento tem, nomeadamente, de: conceber e organizar a sua segurança de acordo com a natureza dos dados pessoais que detém e os danos que possam resultar de uma violação da segurança; ser claro quanto à pessoa pertencente à sua organização incumbida de assegurar a segurança da informação; garantir que dispõe da devida segurança física e técnica, apoiada por políticas e procedimentos robustos, bem como funcionários bem formados; e estar pronto para dar uma resposta célere e eficaz a qualquer violação da segurança.

([93]) N.º 221 das notas explicativas do DPA 2018 (ver nota de rodapé 45).

([94]) A *section 67(4)* do DPA 2018 determina que a notificação tem de incluir uma descrição da natureza da violação dos dados pessoais (incluindo, se possível, as categorias e o número aproximado de titulares de dados afetados, e as categorias e o número aproximado de registos de dados pessoais em causa), o nome e os dados de contacto de um ponto de contacto, uma descrição das consequências prováveis da violação de dados pessoais e uma descrição das medidas adotadas ou propostas pelo responsável pelo tratamento para reparar a violação de dados pessoais (incluindo, se for caso disso, medidas para atenuar eventuais efeitos negativos).

([95]) *Section 67(2)* do DPA 2018.

([96]) *Section 67(6)* do DPA 2018.

([97]) *Section 67(9)* do DPA 2018.

([98]) Nos termos da *section 68(7)* do DPA 2018, o responsável pelo tratamento pode limitar, total ou parcialmente, a prestação de informação ao titular dos dados na medida e enquanto a limitação constitua, tendo em consideração os direitos fundamentais e interesses legítimos do titular dos dados, uma medida necessária e proporcionada para a) evitar prejudicar os inquéritos, as investigações ou os procedimentos judiciais; b) evitar prejudicar a prevenção, a deteção, a investigação ou a repressão de infrações penais, ou a execução de sanções penais; c) proteger a segurança pública; d) proteger a segurança nacional; e) proteger os direitos e liberdades de terceiros.

([99]) *Section 68(3)* do DPA 2018.

([100]) *Section 68(5)* do DPA 2018.

([101]) *Section 68(6)* do DPA 2018, sob reserva da limitação prevista na *section 68(8)* do DPA 2018.

2.4.6. *Transparência*

(55) Os titulares dos dados têm de ser informados sobre as principais características do tratamento dos respetivos dados pessoais. Este princípio da proteção de dados é espelhado na *section 44* do DPA 2018, que, à semelhança do artigo 13.º da Diretiva (UE) 2016/680, determina que o responsável pelo tratamento tem um dever geral de disponibilizar aos titulares dos dados informações sobre o tratamento dos seus dados pessoais (disponibilizando as informações de modo geral ao público ou de qualquer outra forma) ([102]). As informações cuja disponibilização é exigida incluem a) a identidade e os contactos do responsável pelo tratamento; b) se for aplicável, os contactos do encarregado da proteção de dados; c) as finalidades para as quais o responsável pelo tratamento trata os dados pessoais; d) a existência dos direitos de solicitar ao responsável pelo tratamento acesso aos dados pessoais, a retificação dos dados pessoais e o apagamento dos dados pessoais ou a limitação do seu tratamento; e e) a existência do direito de apresentar reclamação junto do comissário para a informação e os contactos do comissário ([103]).

(56) Em casos específicos para permitir o exercício dos direitos dos titulares dos dados ao abrigo do DPA 2018 (por exemplo, quando os dados pessoais objeto de tratamento foram recolhidos sem conhecimento dos titulares dos dados), o responsável pelo tratamento também tem de facultar aos titulares dos dados informações sobre a) o fundamento jurídico do tratamento; b) informações sobre o prazo de conservação dos dados pessoais ou, se tal não for possível, sobre os critérios aplicados para definir esse período; c) se aplicável, informações sobre as categorias de destinatários dos dados pessoais (inclusive nos países terceiros ou nas organizações internacionais); d) as informações necessárias para permitir o exercício dos direitos dos titulares dos dados ao abrigo da parte 3 do DPA 2018 ([104]).

2.4.7. *Direitos individuais*

(57) Tem de ser concedido aos titulares dos direitos um conjunto de direitos executórios. A parte 3, capítulo 3, do DPA 2018 concede às pessoas singulares os direitos de acesso, retificação e apagamento e limitação ([105]), que são comparáveis aos previstos no capítulo III da Diretiva (UE) 2016/680.

(58) O direito de acesso está previsto na *section 45* do DPA 2018. Em primeiro lugar, as pessoas têm o direito de obter uma confirmação por parte do responsável pelo tratamento de que os seus dados pessoais estão a ser ou não objeto de tratamento ([106]). Em segundo lugar, se os dados pessoais são objeto de tratamento, o titular dos dados tem o direito de aceder aos dados e receber as informações seguintes sobre o tratamento: a) as finalidades e o fundamento jurídico do tratamento; b) as categorias de dados envolvidos; c) o destinatário a quem os dados foram divulgados; d) o período de conservação dos dados pessoais; e) a existência do direito do titular dos dados de solicitar a retificação e o apagamento de dados pessoais; f) o direito de apresentar reclamação; e g) qualquer informação sobre a origem dos dados pessoais em causa ([107]).

(59) Em conformidade com a *section 46* do DPA 2018, o titular dos dados tem o direito de exigir ao responsável pelo tratamento que retifique dados pessoais inexatos que lhe digam respeito. O responsável pelo tratamento tem de retificar (ou, se os dados forem inexatos porque estão incompletos, completar) os dados sem demora injustificada. Se os dados pessoais tiverem de ser conservados para efeitos de prova, o responsável pelo tratamento tem de limitar o seu tratamento (em vez de retificar os dados pessoais) ([108]).

([102]) O guia para o tratamento de dados na aplicação da lei dá o seguinte exemplo: «Dispõe uma notificação de privacidade genérica no seu sítio Web que abrange as informações essenciais da organização, a finalidade para a qual trata os dados pessoais, os direitos dos titulares dos dados e o seu direito de apresentar reclamação junto do comissário para a informação. Recebeu informações de que uma pessoa singular estava presente quando ocorreu uma infração penal. Ao interrogar essa pessoa, tem de facultar a informação genérica, bem como informação adicional, para que ela possa exercer os respetivos direitos. Só pode limitar as legítimas informações sobre o tratamento se tal for suscetível de afetar negativamente a investigação que empreende» [*Guide to Law Enforcement Processing, «What information should we supply to an individual?»* (guia para o tratamento de dados na aplicação da lei. «Que informações devemos prestar às pessoas singulares?»], disponível na seguinte ligação: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/the-right-to-be-informed/#ib3).

([103]) Segundo o guia para o tratamento de dados na aplicação da lei, as informações facultadas sobre o tratamento de dados pessoais têm de ser concisas, inteligíveis e de fácil acesso; redigidas em linguagem clara e simples, adaptada às necessidades das pessoas vulneráveis, como as crianças; e gratuitas [*Guide to Law Enforcement Processing, «How should we provide this information?»* (guia para o tratamento de dados na aplicação da lei, «Como devemos prestar essas informações?»), disponível na seguinte ligação: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/the-right-to-be-informed/#ib1].

([104]) *Section 44(2)* do DPA 2018.

([105]) Para uma análise pormenorizada dos direitos dos titulares ver: *Guide to Law Enforcement Processing*, na parte relativa aos direitos individuais, disponível na seguinte ligação: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/

([106]) *Section 45(1)* do DPA 2018.

([107]) *Section 45(2)* do DPA 2018.

([108]) *Section 46(4)* do DPA 2018.

(60) A *section 47* do DPA 2018 determina que as pessoas têm o direito ao apagamento ou à limitação do tratamento. O responsável pelo tratamento tem de apagar ([109]) os dados pessoais sem demora injustificada se o tratamento dos dados pessoais infringir qualquer dos princípios da proteção de dados, o fundamento jurídico do tratamento ou as garantias relacionadas com o arquivo e o tratamento de dados sensíveis. O responsável pelo tratamento tem igualmente de apagar os dados se a tal estiver legalmente obrigado. Se os dados pessoais tiverem de ser conservados para efeitos de prova, o responsável pelo tratamento tem de limitar o seu tratamento (em vez de apagar os dados pessoais) ([110]). O responsável pelo tratamento tem de limitar o tratamento dos dados pessoais se o titular dos dados contestar a exatidão dos dados pessoais, mas não for possível apurar se os dados são exatos ou não ([111]).

(61) Se o titular dos dados solicitar a retificação ou o apagamento de dados pessoais ou a limitação do seu tratamento, o responsável pelo tratamento tem de informar por escrito o titular dos dados do deferimento do pedido ou, caso tenha sido indeferido, informar o titular dos dados dos motivos do indeferimento e das vias de recurso disponíveis [o direito do titular dos dados de solicitar uma investigação por parte do comissário para a informação para apurar se a limitação foi aplicada de modo lícito, o direito a apresentar reclamação junto do comissário para a informação e o direito de requerer uma ordem de cumprimento (*compliance order*) junto de um tribunal] ([112]).

(62) Caso retifique os dados pessoais recebidos de outra autoridade competente, o responsável pelo tratamento tem de notificar a outra autoridade ([113]). Caso retifique ou apague dados pessoais que tenham sido divulgados pelo responsável pelo tratamento ou limite o seu tratamento, o responsável pelo tratamento tem de notificar os destinatários e os destinatários têm igualmente de retificar ou apagar os dados pessoais ou limitar o seu tratamento (desde que tal seja da sua responsabilidade) ([114]).

(63) Além disso, o titular dos dados tem o direito de ser informado pelo responsável pelo tratamento sem demora injustificada sobre as violações dos dados pessoais suscetíveis de resultarem num elevado risco para os direitos e as liberdades das pessoas singulares ([115]).

(64) Em relação a todos os direitos do titular dos dados e à semelhança do previsto no artigo 12.º da Diretiva (UE) 2016/680, o responsável pelo tratamento tem a obrigação de assegurar que qualquer informação ao titular dos dados é fornecida de uma forma concisa, inteligível e de fácil acesso ([116]) e, se possível, deve ser fornecida na mesma forma que o pedido ([117]). O responsável pelo tratamento tem de dar resposta ao pedido do titular dos dados sem demora injustificada e em todo o caso, em princípio, antes do fim do prazo de um mês a contar da data do pedido ([118]). Se tiver dúvidas razoáveis quanto à identidade de uma pessoa, o responsável pelo tratamento pode solicitar informações adicionais e adiar o seguimento do pedido até apurar a identidade. O responsável pelo tratamento pode exigir o pagamento de uma taxa razoável ou indeferir o pedido se considerar que este é manifestamente infundado ([119]). O ICO forneceu uma orientação sobre as circunstâncias em que se considera que um pedido é manifestamente infundado ou excessivo e em que se pode exigir o pagamento de uma taxa ([120]).

(65) Além disso, ao abrigo da *section 53(4)* do DPA 2018, o ministro da tutela pode especificar por meio de regulamentação o montante máximo da taxa.

([109]) Os titulares dos dados podem solicitar ao responsável pelo tratamento que apague os dados pessoais ou limite o seu tratamento (mas os deveres do responsável pelo tratamento de apagar os dados ou limitar o seu tratamento são aplicáveis independentemente de o pedido ter sido apresentado).

([110]) *Sections 46(4)* e *47(2)* do DPA 2018.

([111]) *Section 47(3)* do DPA 2018.

([112]) *Section 48(1)* do DPA 2018.

([113]) *Section 48(7)* do DPA 2018.

([114]) *Section 48(9)* do DPA 2018.

([115]) *Section 68* do DPA 2018.

([116]) *Section 52(1)* do DPA 2018.

([117]) *Section 52(3)* do DPA 2018.

([118]) Segundo a *section 54* do DPA 2018, por «prazo aplicável» entende-se o prazo de um mês, ou outro prazo mais longo especificado nas disposições regulamentares, com início na data pertinente [quando o responsável pelo tratamento recebe o pedido em causa; quando o responsável pelo tratamento recebe as informações solicitadas (caso existam) em relação a um pedido ao abrigo da *section 52(4)* do DPA; ou quando é paga a taxa cobrada (caso exista) em relação ao pedido ao abrigo da *section 53* do DPA].

([119]) *Section 53(1)* do DPA 2018.

([120]) De acordo com a orientação do ICO, o responsável pelo tratamento pode decidir exigir ao titular dos dados o pagamento de taxas se o seu pedido for manifestamente infundado ou excessivo, mas, ainda assim, decidir dar resposta ao mesmo. A taxa tem de ser razoável e justificável em termos de custo. *Guide to Law Enforcement Processing, «Manifestly unfounded and excessive requests»* (guia para o tratamento de dados na aplicação da lei, «Pedidos manifestamente infundados e excessivos», disponível na seguinte ligação: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/manifestly-unfounded-and-excessive-requests/

2.4.7.1. Limitações dos direitos do titular dos dados e obrigações em matéria de transparência

(66) As autoridades competentes podem, em determinadas circunstâncias, limitar determinados direitos do titular de dados: o direito de acesso ([121]), a ser informado ([122]), a ter conhecimento das violações de dados pessoais ([123]) e a ser informado sobre os motivos de indeferimento de um pedido de retificação ou apagamento ([124]). À semelhança do regime constante do capítulo III da Diretiva (UE) 2016/680, a autoridade competente, tendo em conta os direitos fundamentais e os interesses legítimos do titular dos dados, só pode aplicar a limitação se esta for necessária e proporcionada para: a) evitar prejudicar um inquérito, uma investigação ou um procedimento oficial ou judicial; b) evitar prejudicar a prevenção, a deteção, a investigação ou a repressão de infrações penais, ou a execução de sanções penais; c) proteger a segurança pública; d) proteger a segurança nacional; e) proteger os direitos e liberdades de terceiros.

(67) O ICO forneceu uma orientação sobre a aplicação destas limitações. De acordo com esta orientação, os responsáveis pelo tratamento têm de realizar uma análise caso a caso para alcançar um equilíbrio entre os direitos da pessoa em causa e o eventual prejuízo decorrente da divulgação. Mais particularmente, têm de justificar o caráter necessário e proporcionado de qualquer limitação aplicada e só podem limitar o que é fornecido se tal prejudicar as finalidades mencionadas acima ([125]).

(68) Existe ainda um conjunto de outras orientações emitidas pelas autoridades competentes que fornecem informações pormenorizadas sobre todos os aspetos da legislação em matéria de proteção de dados, incluindo sobre a aplicação das limitações dos direitos dos titulares dos dados ([126]). Por exemplo, no que respeita à *section 45(4)*, segundo o manual para a proteção de dados do *National Police Chiefs' Counsel*: «É importante salientar que as limitações só podem ser aplicadas na medida do necessário e enquanto forem necessárias. Por conseguinte, é proibida uma aplicação geral da limitação a todos os dados pessoais de um requerente ou uma aplicação permanente da limitação. Quanto a este último caso, muitas vezes é necessário impedir a divulgação dos dados pessoais recolhidos sem o conhecimento do titular dos dados sob suspeita numa investigação para evitar prejudicar a investigação no decurso da mesma, mas, posteriormente, não adviria prejuízo algum se os dados pessoais fossem divulgados à pessoa em causa durante o interrogatório. As forças policiais têm de adotar processos que assegurem que a aplicação destas limitações se limita unicamente à medida do necessário e pelo prazo necessário» ([127]). Esta orientação também fornece exemplos das circunstâncias em que é mais provável que se recorra a cada uma das limitações ([128]).

(69) Além disso, no que se refere à possibilidade de limitar qualquer um dos direitos mencionados acima para efeitos de proteção da «segurança nacional», o responsável pelo tratamento pode solicitar um certificado assinado por um ministro do Gabinete ou pelo Procurador-Geral (ou *Advocate General* na Escócia) que ateste que a limitação desses direitos constitui uma medida necessária e proporcionada para a proteção da segurança nacional ([129]). O Governo do Reino Unido emitiu uma orientação sobre os certificados de segurança nacional ao abrigo do DPA 2018 que, nomeadamente, destaca que qualquer limitação dos direitos dos titulares dos dados para salvaguardar a segurança nacional tem de ser proporcionada e necessária ([130]) (para mais pormenores sobre os certificados de segurança nacional, ver considerandos 131 a 134).

([121]) *Section 45(4)* do DPA 2018.
([122]) *Section 44(4)* do DPA 2018.
([123]) *Section 68(7)* do DPA 2018.
([124]) *Section 48(3)* do DPA 2018.
([125]) Ver, por exemplo, *Guide to Law Enforcement Processing*, na parte respeitante ao direito de acesso, disponível na seguinte ligação: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/individual-rights/the-right-of-access/#ib8
([126]) Ver, por exemplo, *Data Protection Manual for Police Data Protection Professionals*, emitido pelo *National Police Chiefs' Counsel* (ver nota de rodapé 27), ou a orientação publicada pelo *Serious Fraud Office*, disponível na seguinte ligação: https://www.sfo.gov.uk/publications/guidance-policy-and-protocols/sfo-operational-handbook/data-protection/
([127]) *Data Protection Manual* do *National Police Chiefs' Counsel*, p. 140 (ver nota de rodapé 27).
([128]) O manual de proteção de dados do *National Police Chiefs' Counsel* determina que a finalidade de «evitar prejudicar um inquérito, uma investigação ou um procedimento oficial ou judicial» é suscetível de ter relevância no caso dos dados pessoais tratados em inquéritos, processos do tribunal de família, investigações disciplinares internas em matéria não penal e investigações como a Investigação independente aos abusos sexuais de menores; ao passo que a finalidade de «proteger os direitos e liberdades de terceiros» é pertinente para os dados pessoais relacionados igualmente com outras pessoas e com o requerente» (Data Protection Manual do National Police Chiefs' Counsel, p. 140, ver nota de rodapé 27).
([129]) *Section 79* do DPA 2018.
([130]) *UK Government Guidance on National Security Certificates* (orientações do Governo do Reino Unido sobre os certificados de segurança nacional), 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

(70) Além disso, se for aplicável uma limitação dos direitos dos titulares dos dados, a autoridade competente tem de informar o titular dos dados sem demora injustificada de que os seus direitos foram limitados, dos motivos subjacentes à limitação e das vias de recurso disponíveis, exceto se a prestação de tais informações prejudicar os motivos subjacentes à aplicação da limitação ([131]). Como medida de salvaguarda adicional contra a incorreta utilização das limitações, o responsável pelo tratamento tem de registar os motivos subjacentes à limitação da informação e disponibilizar o registo ao comissário para a informação se solicitado ([132]).

(71) Se o responsável pelo tratamento se recusar a prestar informações adicionais em matéria de transparência ou a proporcionar o acesso, ou indeferir um pedido de retificação, apagamento ou limitação do tratamento, a pessoa singular pode solicitar ao comissário para a informação que investigue se o responsável pelo tratamento tem utilizado a limitação de modo lícito ([133]). A pessoa singular em causa também pode apresentar reclamação ao comissário para a informação ou requerer que um tribunal ordene que o responsável pelo tratamento dê seguimento ao pedido ([134]).

2.4.7.2. Decisões automatizadas

(72) As *sections 49* e *50* do DPA 2018 abrangem, respetivamente, os direitos relacionados com as decisões automatizadas e as garantias a aplicar ([135]). À semelhança do artigo 11.º da Diretiva (UE) 2016/680, o responsável pelo tratamento só pode tomar uma decisão significativa exclusivamente com base no tratamento automatizado de dados pessoais se tal for exigido ou autorizado por lei ([136]). Uma decisão é considerada significativa se produzir um efeito legal adverso respeitante ao titular dos dados ou se afetar significativamente o titular dos dados ([137]).

(73) Se o responsável pelo tratamento estiver obrigado ou for autorizado por lei a tomar uma decisão significativa, a *section 50* do DPA 2018 estabelece as garantias aplicáveis a tal decisão (denominada «decisão significativa elegível»). Logo que seja razoavelmente exequível, o responsável pelo tratamento tem de notificar o titular dos dados da tomada de tal decisão. Posteriormente, o titular dos dados pode requerer, no prazo de um mês, a reapreciação da decisão ou a tomada de uma nova decisão que não se baseie unicamente no tratamento automatizado. O responsável pelo tratamento tem de analisar o pedido e informar o titular dos dados do resultado da referida análise. O DPA 2018 confere ao ministro da tutela o poder de adotar regulamentação relativa a garantias adicionais ([138]). Até ao momento não foi adotada regulamentação para o efeito.

2.4.8. *Transferências ulteriores*

(74) O nível de proteção conferido aos dados pessoais transferidos a partir de uma autoridade de aplicação da lei de um Estado-Membro para uma autoridade de aplicação da lei do Reino Unido não pode ser prejudicado pela transferência subsequente desses dados para destinatários num país terceiro. As referidas «transferências ulteriores», que constituem, da perspetiva da autoridade de aplicação da lei 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 britânica.

([131]) *Section 44(5)* e *(6)*; *Section 45(5)* e *(6)*; *Section 48(4)* do DPA 2018.
([132]) *Section 44(7)*; *Section 45(7)*; *Section 48(6)* do DPA 2018.
([133]) *Section 51* do DPA 2018.
([134]) *Section 167* do DPA 2018.
([135]) No que respeita ao alcance do tratamento automatizado, as notas explicativas do DPA 2018 determinam que: «estas disposições dizem respeito às decisões totalmente automatizadas e não ao tratamento automatizado. O tratamento automatizado (incluindo a definição de perfis) trata-se de uma operação realizada sobre os dados sem necessidade de intervenção humana. É utilizado com regularidade na aplicação da lei para separar grandes conjuntos de dados em quantidades razoáveis para posterior utilização por um operador humano. As decisões automatizadas são uma forma de tratamento automatizado e exigem que a decisão final seja tomada sem interferência humana». (Notas explicativas do DPA, n.º 204, ver nota de rodapé 45).
([136]) Para além da proteção prevista no DPA, existem outras limitações legislativas no quadro jurídico do Reino Unido que são aplicáveis às autoridades de aplicação da lei e preveniriam o tratamento automatizado (incluindo a definição de perfis) que resulte na discriminação ilícita. O *Human Rights Act 1998* incorpora os direitos da CEDH no direito do Reino Unido, nomeadamente o direito consagrado no artigo 14.º da Convenção, a proibição da discriminação. Analogamente, o *Equality Act 2010* proíbe a discriminação contra as pessoas com características protegidas (nomeadamente, o sexo, a raça, a deficiência, etc.).
([137]) *Section 49(2)* do DPA 2018.
([138]) *Section 50(4)* do DPA 2018.

(75) O regime do Reino Unido em matéria de transferências internacionais é regulamentado pela parte 3, capítulo 5, do DPA 2018 ([139]) e reflete a abordagem adotada no capítulo V da Diretiva (UE) 2016/680. Mais particularmente, para transferir dados pessoais para um país terceiro, a autoridade competente tem de cumprir três condições: a) a transferência tem de ser necessária para efeitos de aplicação da lei; b) a transferência tem de se basear: i) num regulamento de adequação respeitante ao país terceiro, ii) se não se basear num regulamento de adequação, na existência de garantias adequadas, ou iii) se não se basear num regulamento de adequação nem em garantias adequadas, tem de basear-se em circunstâncias especiais; e c) o destinatário da transferência tem de ser: i) uma autoridade relevante (ou seja, a autoridade equivalente a uma autoridade competente) no país terceiro, ii) uma «organização internacional relevante», por exemplo, um órgão internacional que desempenha funções correspondentes a qualquer uma das finalidades de aplicação da lei, ou iii) uma pessoa que não uma autoridade relevante, mas unicamente se a transferência for estritamente necessária para a consecução de uma das finalidades de aplicação da lei; os direitos e liberdades fundamentais do titular dos dados não se sobrepõem ao interesse público que obriga à transferência; uma transferência dos dados pessoais para uma autoridade relevante no país terceiro seria ineficaz ou inadequada; e o destinatário foi informado das finalidades para as quais os dados podem ser tratados ([140]).

(76) Os regulamentos de adequação respeitantes a um país terceiro, um território ou um setor de um país terceiro, uma organização internacional ou uma descrição ([141]) desse país, território, setor ou organização são adotados pelo ministro da tutela. No que respeita ao critério a cumprir, o ministro da tutela tem de avaliar se o referido território/ /setor/organização garante um nível adequado de proteção dos dados pessoais. A *section 74A(4)* do DPA 2018 especifica que, para o efeito, o ministro da tutela tem de considerar um conjunto de elementos que reflete os constantes do artigo 36.º da Diretiva (UE) 2016/680 ([142]). A este respeito, desde o fim do período de transição, a parte 3 do DPA 2018 constitui «legislação interna derivada da UE», que, tal como explicado, será interpretada pelos tribunais do Reino Unido em conformidade com a jurisprudência pertinente do Tribunal de Justiça antes da saída do Reino Unido da União e os princípios gerais do direito da União, tal como vigoravam imediatamente antes do fim do período de transição. Tal inclui o critério da «equivalência essencial» que será, por conseguinte, aplicado às avaliações de adequação realizadas pelas autoridades do Reino Unido.

(77) Quanto ao procedimento, os regulamentos estão sujeitos aos requisitos processuais «gerais» previstos na *section 182* do DPA 2018. Ao abrigo deste procedimento, o ministro da tutela tem de consultar o comissário para a informação

([139]) Este novo regime surgiu no fim do período de transição, incluindo o poder concedido ao ministro da tutela para adotar regulamentos de adequação. No entanto, os Regulamentos DPPEC (em particular, o *schedule 21*, n.os 10 a 12, que este regulamento insere no DPA 2018) determina que determinadas transferências de dados pessoais durante e após o período de transição são tratadas como se se baseassem em regulamentos de adequação. Estas transferências incluem transferências para países terceiros sujeitos a uma decisão de adequação da UE no fim do período de transição e para os Estados-Membros da UE, os Estados da EFTA e o território de Gibraltar em virtude da aplicação da Diretiva Proteção de Dados na Aplicação da Lei ao tratamento de dados para fins de aplicação da lei [os Estados da EFTA aplicam a Diretiva (UE) 2016/680 devido às obrigações que lhes incumbem por força das disposições do acervo de Schengen]. Tal significa que no fim do período de transição as transferências para estes países podem prosseguir tal como antes da saída da UE. Após o fim do período de transição, o ministro da tutela tem de proceder a uma análise destas conclusões de adequação no prazo de quatro anos.

([140]) *Sections 73* e *77* do DPA 2018.

([141]) 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 limitações específicas (por exemplo, um regulamento de adequação relativo a apenas determinados tipos de transferências de dados).

([142]) Ver *section 74A(4)* do DPA 2018, que determina que, ao avaliar a adequação do nível de proteção «o ministro da tutela tem, em particular, de ter em conta a) o princípio do Estado de direito, o respeito dos direitos humanos e das liberdades fundamentais, a legislação pertinente, tanto geral como setorial, incluindo em matéria de segurança pública, defesa, segurança nacional e de direito penal e o acesso das autoridades públicas aos dados pessoais, bem como a aplicação de tal legislação, regras de proteção de dados, regras profissionais e medidas de segurança, incluindo regras para a transferência ulterior de dados pessoais para outro país terceiro ou organização internacional, que são cumpridas nesse país ou nessa organização internacional, jurisprudência, bem como direitos efetivos e executórios do titular de dados e vias de recurso administrativo e judicial para os titulares de dados cujos dados tenham sido transferidos, b) a existência e funcionamento efetivo de uma ou mais autoridades de controlo independentes no país terceiro ou a que a organização internacional está sujeita, responsável por assegurar o cumprimento das regras de proteção dos dados, incluindo poderes coercivos adequados, para assistir e aconselhar os titulares de dados no exercício dos seus direitos e para cooperar com o comissário, e c) os compromissos internacionais assumidos pelo país terceiro ou pela organização internacional em causa ou outras obrigações decorrentes de convenções ou instrumentos juridicamente vinculativos, bem como da sua participação em sistemas multilaterais ou regionais, em particular no que respeita à proteção dos dados pessoais».

ao propor futuros regulamentos de adequação do Reino Unido ([143]). Depois de adotados pelo ministro da tutela, esses regulamentos são apresentados ao parlamento e sujeitos ao procedimento de «resolução negativa», segundo o qual as câmaras do parlamento podem examinar o regulamento e podem aprovar uma moção para anular o regulamento no prazo de 40 dias ([144]).

(78) Nos termos da *section 74B(1)* do DPA 2018, os regulamentos de adequação devem ser revistos, no máximo, de quatro em quatro anos, devendo o ministro da tutela controlar, de forma continuada, os desenvolvimentos nos países terceiros e nas organizações internacionais suscetíveis de afetarem as decisões que visam criar regulamentos de adequação ou alterar ou revogar esses regulamentos. Caso tenha conhecimento de que um determinado país ou uma organização deixou de assegurar um nível adequado de proteção de dados pessoais, o ministro da tutela tem de alterar ou revogar, na medida do necessário, 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.

(79) À semelhança do disposto no artigo 37.º da Diretiva (UE) 2016/680, na falta de uma decisão de adequação, seria possível proceder a uma transferência de dados pessoais no contexto da aplicação da lei se existissem garantias adequadas. Tais garantias são asseguradas por meio de a) um instrumento jurídico vinculativo que contém garantias adequadas para a proteção de dados pessoais; ou b) uma avaliação realizada pelo responsável pelo controlo, que, tendo avaliado todas as circunstâncias inerentes à transferência, conclui que existem garantias adequadas para proteger os dados ([145]). Além disso, quando as transferências se baseiam em garantias adequadas, o DPA 2018 prevê que, além da função de supervisão habitual do ICO, as autoridades competentes têm de prestar informações específicas sobre as transferências para o ICO ([146]).

(80) Caso não tenha por base uma decisão de adequação ou garantias adequadas, a transferência só pode ser efetuada em circunstâncias determinadas e específicas, denominadas «circunstâncias especiais» ([147]). É esse o caso quando a transferência é necessária: a) para proteger os interesses vitais do titular dos dados ou de outra pessoa; b) para proteger os interesses legítimos do titular dos dados; c) para prevenir uma ameaça imediata e grave contra a segurança pública de um país terceiro; d) em determinados casos para efeitos de aplicação da lei; ou e) em determinados casos por um motivo legal (como seja os relacionados com processos judiciais ou para obter aconselhamento jurídico) ([148]). Convém salientar que as alíneas d) e e) não são aplicáveis caso os direitos e as liberdades do titular dos dados se sobreponham ao interesse público da transferência ([149]). Este conjunto de circunstâncias corresponde às situações e condições específicas consideradas «derrogações» ao abrigo do artigo 38.º da Diretiva (UE) 2016/680.

(81) Nestas circunstâncias, a data, a hora e a justificação da transferência, o nome e quaisquer outras informações pertinentes sobre o destinatário e uma descrição dos dados pessoais transferidos têm de ser documentados e transmitidos ao comissário para a informação mediante pedido ([150]).

(82) A *section 78* do DPA 2018 regulamenta o cenário das «transferências subsequentes», ou seja, quando os dados pessoais que foram transferidos do Reino Unido para um país terceiro são subsequentemente transferidos para outro país terceiro ou uma organização internacional. Nos termos da *section 78(1)* do DPA, o responsável pelo tratamento britânico tem de condicionar a transferência dos dados à proibição de outras transferências para um país terceiro sem a autorização do responsável pelo tratamento que procede à transferência. Além disso, de acordo com a *section 78(3)*, e à semelhança do disposto no artigo 35.º, n.º 1, alínea e), da Diretiva (UE) 2016/680, são aplicáveis

([143]) Ver o memorando de entendimento entre o ministro 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

([144]) Durante este período de 40 dias, ambas as câmaras do parlamento podem votar contra os regulamentos, se assim o desejarem; se a moção for aprovada, em última instância, os regulamentos deixarão de ter efeito jurídico.

([145]) *Section 75* do DPA 2018.

([146]) Nos termos da *section 75(3)* do DPA 2018, no caso de uma transferência de dados pessoais dependente de garantias adequadas: a) a transferência tem de ser documentada, b) a documentação tem de ser transmitida ao comissário mediante pedido e c) a documentação tem de incluir, em particular, i) a data e hora de transferência, ii) o nome e quaisquer outras informações pertinentes sobre o destinatário, iii) a justificação da transferência e iv) uma descrição dos dados pessoais transferidos.

([147]) *Guide to Law Enforcement Processing, «Are there any special circumstances?»* (guia para o tratamento de dados na aplicação da lei, «Existem circunstâncias especiais?»), disponível na seguinte ligação: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/international-transfers/#ib3).

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

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

([150]) *Section 76(3)* do DPA 2018.

diversos requisitos essenciais caso seja exigida essa autorização. Mais especificamente, ao decidir se uma transferência deve ser autorizada ou não, a autoridade competente tem de assegurar que a transferência posterior é necessária para efeitos de aplicação da lei e deve considerar, entre outros fatores, a) a gravidade das circunstâncias que conduziram ao pedido de autorização, b) a finalidade para a qual os dados pessoais foram inicialmente transferidos e c) as normas de proteção dos dados pessoais aplicáveis no país terceiro ou na organização internacional para a qual os dados pessoais seriam transferidos.

(83) Além disso, são aplicáveis salvaguardas adicionais quando os dados objeto de transferência posterior a partir do Reino Unido tenham sido transferidos inicialmente a partir da União Europeia.

(84) Em primeiro lugar, a *section 73(1)(b)* do DPA 2018 — à semelhança, do artigo 35.º, n.º 1, alínea c), da Diretiva (UE) 2016/680 — determina que, caso os dados pessoais tenham sido inicialmente transmitidos ou disponibilizados de outra forma ao responsável pelo tratamento ou outra autoridade competente por um Estado-Membro, esse Estado-Membro, ou qualquer pessoa estabelecida nesse Estado-Membro que seja uma autoridade competente para efeitos da Diretiva (UE) 2016/680, tem de ter autorizado a transferência em conformidade com a legislação do Estado-Membro.

(85) No entanto, à semelhança do artigo 35.º, n.º 2, da Diretiva (UE) 2016/680, não é necessária esta autorização se a) a transferência for necessária para prevenir uma ameaça imediata e grave à segurança pública de um Estado-Membro ou de um país terceiro ou aos interesses essenciais de um Estado-Membro e c) o consentimento não puder ser obtido em tempo útil. Neste caso, a autoridade do Estado-Membro que seria responsável por tomar uma decisão sobre a autorização da transferência tem de ser informada sem demora ([151]).

(86) Em segundo lugar, aplica-se a mesma abordagem caso os dados tenham sido inicialmente transferidos a partir da União Europeia para o Reino Unido e, de novo, transferidos pelo Reino Unido para um país terceiro que, subsequentemente, procederia a uma transferência ulterior para um país terceiro. Neste caso, nos termos da *section 78(4)*, a autoridade competente do Reino Unido não pode autorizar esta última transferência, ao abrigo da *section 78(1)*, salvo se «o Estado-Membro [que tenha transferido inicialmente os dados em questão], ou qualquer pessoa estabelecida nesse Estado-Membro que seja uma autoridade competente para efeitos da Diretiva Proteção de Dados na Aplicação da Lei, tenha autorizado a transferência em conformidade com o direito do Estado-Membro». Estas salvaguardas são importantes já que permitem às autoridades dos Estados-Membros assegurar a continuidade da proteção, em conformidade com o direito da UE em matéria de proteção de dados, ao longo da «cadeia de transferências».

(87) Este novo quadro para transferências internacionais tornou-se aplicável no fim do período de transição ([152]). Contudo, o *schedule 21*, n.ºs 10 a 12, do DPA 2018 (introduzido pelos Regulamentos DPPEC) prevê que, no fim do período de transição, determinadas transferências de dados pessoais sejam tratadas como se se baseassem em regulamentos de adequação. Estas transferências incluem transferências para um Estado-Membro, um Estado da EFTA, um país terceiro sujeito a uma decisão de adequação da UE no fim do período de transição e o território de Gibraltar. Consequentemente, as transferências para esses países podem continuar como ocorriam antes da saída do Reino Unido da União. Após o fim do período de transição, o ministro da tutela tem de 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 pertinentes não deixarão automaticamente de ter efeito se a análise não for concluída até ao fim de dezembro de 2024.

2.4.9. *Responsabilidade*

(88) De acordo com o princípio da responsabilidade, as autoridades públicas que procedem ao 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.

(89) Este princípio é espelhado na *section 56* do DPA 2018, que introduz uma obrigação de responsabilidade geral do responsável pelo tratamento, ou seja, uma obrigação de aplicar medidas técnicas e organizativas adequadas para assegurar e poder demonstrar que o tratamento de dados pessoais cumpre os requisitos da parte 3 do DPA 2018. As medidas aplicadas têm de ser reavaliadas e atualizadas se necessário e, sempre que tal se afigure proporcionado no que respeita ao tratamento, incluir políticas adequadas de proteção dos dados.

([151]) *Section 73(5)* do DPA 2018.

([152]) No que respeita à aplicabilidade deste novo quadro, há que lê-lo 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-Reino Unido»), disponível na seguinte ligação: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:22020A1231(01)&from=PT

(90) Em consonância com o capítulo IV da Diretiva (UE) 2016/680, as *sections 55* a *71* do DPA 2018 preveem diversos mecanismos para assegurar a responsabilidade e permitir aos responsáveis pelo tratamento e subcontratantes comprovar a sua conformidade. Mais particularmente, os responsáveis pelo tratamento estão obrigados a aplicar medidas de proteção de dados desde a conceção e por predefinição, ou seja, a assegurar a eficaz aplicação dos princípios da proteção de dados, e são obrigados a manter registos de todas as categorias de atividades de tratamento da responsabilidade do responsável pelo tratamento (incluindo informações sobre a identidade do responsável pelo tratamento, os dados de contacto do encarregado da proteção de dados, as finalidades do tratamento, as categorias de destinatários das divulgações e uma descrição das categorias dos titulares dos dados e dados pessoais) e disponibilizar estes registos ao comissário para a informação mediante pedido. O responsável pelo tratamento e subcontratante têm igualmente de manter registos cronológicos de determinadas operações de tratamento e disponibilizá-los ao comissário para a informação ([153]). Os responsáveis pelo tratamento também estão especificamente obrigados a cooperar com o comissário para a informação no desempenho das atribuições do comissário.

(91) O DPA 2018 também estabelece requisitos adicionais para o tratamento suscetível de resultar num elevado risco para os direitos e as liberdades das pessoas singulares. Estes incluem uma obrigação de realizar avaliações de impacto relativas à proteção de dados e consultar o comissário para a informação antes do tratamento se uma avaliação indicar que o tratamento resultaria num elevado risco para os direitos e as liberdades das pessoas singulares (na ausência de medidas de atenuação do risco).

(92) Os responsáveis pelo tratamento têm, além disso, de nomear um encarregado da proteção de dados, a menos que o responsável pelo tratamento seja um tribunal, ou outra autoridade judiciária, no exercício da sua competência judicial ([154]). O responsável pelo tratamento tem de assegurar que o encarregado da proteção de dados participa em todas as questões relacionadas com a proteção dos dados pessoais, dispõe dos recursos e do acesso necessário aos dados pessoais e às operações de tratamento e pode desempenhar as suas funções de forma independente. As funções do encarregado da proteção de dados estão estabelecidas na *section 71* do DPA 2018, incluindo prestar informações e aconselhamento e fiscalizar a conformidade, bem como cooperar e servir de ponto de contacto com o comissário para a informação. No desempenho das suas funções, o encarregado da proteção de dados tem de ter em consideração os riscos associados às operações de tratamento, tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento.

2.5. **Supervisão e aplicação coerciva**

2.5.1. *Supervisão independente*

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

(94) No Reino Unido, cabe ao comissário para a informação efetuar a supervisão e a imposição do cumprimento do RGPD do Reino Unido e do DPA 2018 ([155]). O comissário para a informação supervisiona o tratamento de dados pessoais pelas autoridades competentes abrangidas pelo âmbito de aplicação da parte 3 do DPA 2018 ([156]). O comissário para a informação é uma «sociedade individual»: uma entidade jurídica distinta 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 ([157]). O ministério que patrocina o comissário para a informação (*sponsor department*) é o Ministério dos Assuntos Digitais, da Cultura, dos Meios de Comunicação e do Desporto ([158]).

([153]) *Section 62* do DPA 2018.
([154]) *Section 69* do DPA 2018.
([155]) Artigo 36.º, n.º 2, alínea b), da Diretiva (UE) 2016/680.
([156]) *Section 116* do DPA 2018.
([157]) *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
([158]) A relação entre os dois é regulamentada por um acordo de gestão. Mais particularmente, as responsabilidades principais do Ministério dos Assuntos Digitais, da Cultura, dos Meios de Comunicação e do Desporto, enquanto ministério patrocinador, incluem: garantir que o ICO recebe financiamento e recursos adequados; representar os interesses do ICO junto do parlamento e de outros ministérios; garantir a existência de um quadro nacional de proteção de dados sólido; e dar orientação e apoio ao ICO em questões empresariais, como mercado imobiliário, locações e aquisições (o Acordo de Gestão para 2018-2021 está disponível na seguinte ligação: https://ico.org.uk/media/about-the-ico/documents/2259800/management-agreement-2018-2021.pdf).

(95) 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 Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho ([159]). De acordo com o RGPD do Reino Unido, o comissário tem de agir com total independência no desempenho das suas funções e no exercício das suas competências, não pode estar sujeito a influências externas, diretas ou indiretas, no desempenho das suas funções e no exercício das suas competências, e não pode solicitar nem receber instruções de ninguém. O comissário tem igualmente de se abster 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.

(96) 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 pela rainha com base numa recomendação do governo na sequência de um concurso equitativo e aberto. O candidato tem de ter as qualificações, as competências e as aptidões adequadas. De acordo com o *Governance Code on Public Appointments* (código para a governação das nomeações públicas) ([160]), o painel de avaliação consultivo efetua uma lista dos candidatos que podem ser nomeados. Antes de o ministro dos Assuntos Digitais, da Cultura, dos Meios de Comunicação e do Desporto tomar a sua decisão, a comissão especial competente do parlamento tem de realizar uma triagem prévia à nomeação. A posição da comissão é tornada pública ([161]).

(97) O mandato do comissário para a informação dura no máximo sete anos. O comissário para a informação pode ser afastado do cargo pela rainha na sequência de um comunicado de ambas as câmaras do parlamento ([162]). Só pode apresentado um pedido de exoneração do comissário para a informação a uma das câmaras do parlamento se um ministro tiver apresentado um relatório à câmara em causa 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 ([163]).

(98) O financiamento do comissário para a informação provém de três fontes: i) taxas de proteção de dados pagas pelos responsáveis pelo tratamento que são fixadas pelos regulamentos do ministro da tutela ([164]) e representam entre 85 % e 90 % do orçamento anual do gabinete ([165]); ii) a subvenção eventualmente paga pelo governo ao comissário para a informação e que é maioritariamente utilizada para financiar os custos de funcionamento do gabinete do comissário para a informação no que diz respeito a funções não relacionadas com a proteção de dados ([166]); e iii) taxas cobradas pelos serviços ([167]). De momento, essas taxas não são cobradas.

(99) As funções gerais do comissário para a informação relativas ao tratamento de dados pessoais abrangido pelo âmbito de aplicação da parte 3 do DPA 2018 são estabelecidas no *schedule 13* do DPA 2018. As funções incluem o acompanhamento e a aplicação coerciva da parte 3 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

([159]) Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados) (JO L 119 de 4.5.2016, p. 1).

([160]) *Governance Code on Public Appointments*, disponível na seguinte ligação: https://www.gov.uk/government/publications/governance-code-for-public-appointments

([161]) *Second Report of Session 2015-2016* (Segundo relatório da sessão de 2015-2016) da Comissão da Cultura, dos Meios de Comunicação e do Desporto da Câmara dos Comuns, disponível na seguinte ligação: https://publications.parliament.uk/pa/cm201516/cmselect//cmcumeds/990/990.pdf

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

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

([164]) *Section 137* do DPA 2018.

([165]) As *sections 137* e *138* do DPA 2018 incluem uma série de garantias para assegurar a fixação correta das taxas. Mais particularmente, o artigo 137.º, n.º 4, do DPA 2018 enumera as matérias que o ministro da tutela tem de ter em conta ao elaborar regulamentos que especificam o montante que as diferentes organizações têm de pagar. A *section 138(1)* e a *section 182* do DPA 2018 também contêm uma obrigação legal que exige que o ministro da tutela consulte o comissário para a informação e outros representantes das pessoas suscetíveis de serem afetadas pelos regulamentos, antes da respetiva elaboração, para que os seus pontos de vista sejam tidos em conta. Além disso, nos termos da *section 138(2)* do DPA 2018, o comissário para a informação é obrigado a manter o funcionamento dos *Charges Regulations* (Regulamentos relativos a taxas) sob análise e pode apresentar propostas ao ministro da tutela para que sejam efetuadas alterações nos regulamentos. Por último, salvo nos casos em que os regulamentos são elaborados simplesmente para ter em conta um aumento do índice de preços 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 elaborados até terem sido aprovados por resolução por cada uma das câmaras do parlamento.

([166]) O Acordo de Gestão esclareceu que «[o] ministro da tutela pode efetuar pagamentos ao comissário para a informação com os fundos disponibilizados pelo parlamento, nos termos do *schedule 12*, n.º 9, do DPA 2018. Após consulta ao comissário para a informação, o DCMS pagar-lhe-á os montantes adequados (a subvenção) para os custos administrativos do ICO e o exercício das funções do comissário para a informação no que respeita a um conjunto de funções específicas, incluindo a liberdade de informação» (Acordo de Gestão para 2018-2021, ponto 1.12, ver a nota de rodapé 158).

([167]) *Section 134* do DPA 2018.

administrativas, a sensibilização dos responsáveis pelo tratamento e subcontratantes para as suas obrigações, a prestação de informações aos titulares de dados relativamente ao exercício dos seus direitos e a realização de investigações. A fim de assegurar a independência do sistema judiciário, o comissário para a informação não está autorizado a exercer as suas funções quanto ao tratamento de dados pessoais efetuado pelos tribunais ou por pessoas singulares no exercício da sua competência judicial. Todavia, a supervisão do sistema judiciário é assegurada por órgãos especializados, analisados abaixo.

2.5.1.1 Aplicação coerciva, incluindo sanções

(100) O comissário possui poderes gerais de investigação, de correção, de autorização e de aconselhamento no que respeita ao tratamento de dados pessoais a que se aplica a parte 3 do DPA 2018. O comissário tem poder para notificar o responsável pelo tratamento ou o subcontratante de uma alegada violação da parte 3, fazer advertências aos responsáveis pelo tratamento ou ao subcontratante no sentido de que as operações de tratamento previstas são suscetíveis de violar as disposições da parte 3 e fazer repreensões ao responsável pelo tratamento ou ao subcontratante sempre que as operações de tratamento tiverem violado as disposições da parte 3. Além disso, o comissário pode emitir, por iniciativa própria ou a pedido, pareceres dirigidos ao parlamento do Reino Unido, ao governo ou a outras instituições e organismos, bem como ao público, sobre qualquer assunto relacionado com a proteção de dados pessoais ([168]).

(101) Além disso, o comissário tem poderes para:

— ordenar que o responsável pelo tratamento e o subcontratante (e, em determinadas circunstâncias, qualquer outra pessoa) lhe forneçam as informações de que necessite mediante uma notificação informativa («notificação informativa») ([169]),

— realizar investigações e auditorias por meio da emissão de uma notificação de avaliação, o que poderá implicar que o responsável pelo tratamento ou o subcontratante permita que o comissário entre em 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 («notificação de avaliação») ([170]),

— obter acesso de outra forma aos documentos dos responsáveis pelo tratamento e dos subcontratantes e acesso às suas instalações em conformidade com a *section 154* do DPA 2018 («poderes de entrada e inspeção»),

— exercer os poderes de correção por meio de advertências e repreensões ou emitir ordens por meio de uma notificação de execução, que exige que os responsáveis pelo tratamento/subcontratantes tomem ou se abstenham de tomar determinadas medidas («notificação de execução») ([171]), e

— impor coimas sob a forma de uma notificação de sanção («notificação de sanção») ([172]).

(102) A *Regulatory Action Policy* (política de intervenção regulamentar) do ICO descreve as circunstâncias mediante as quais o comissário emite, respetivamente, uma notificação informativa, de avaliação, de execução e de sanção ([173]). A notificação de execução pode impor requisitos que o comissário considera adequados para efeitos de correção do incumprimento. A notificação de sanção exige que a pessoa pague um montante especificado na notificação ao comissário para a informação. A notificação de sanção pode ser emitida sempre que houver um incumprimento de determinadas disposições do DPA 2018 ([174]) ou pode ser emitida a um responsável pelo tratamento ou subcontratante que não tenha respeitado uma notificação informativa, uma notificação de avaliação ou uma notificação de execução.

(103) Mais especificamente, ao determinar se há lugar à emissão de uma notificação de sanção a um responsável pelo tratamento ou subcontratante e ao determinar o montante da sanção, o comissário para a informação tem de ter em conta as matérias constantes da *section 155(3)* do DPA 2018, incluindo a natureza e a gravidade do incumprimento, o caráter intencional ou negligente do incumprimento, todas as medidas tomadas pelo responsável pelo tratamento ou pelo subcontratante para atenuar os danos sofridos pelos titulares dos dados, o nível de

([168]) *Schedule 13*, n.º 2, do DPA 2018.
([169]) *Section 142* do DPA 2018 (sob reserva das limitações previstas na *section 143* do DPA 2018).
([170]) *Section 146* do DPA 2018 (sob reserva das limitações previstas na *section 147* do DPA 2018).
([171]) *Sections 149* a *151* do DPA 2018 (sob reserva das limitações previstas na *section 152* do DPA 2018).
([172]) *Section 155* do DPA 2018 (sob reserva das limitações previstas na *section 156* do DPA 2018).
([173]) *Regulatory Action Policy*, disponível na seguinte ligação: https://ico.org.uk/media/about-the-ico/documents/2259467/regulatory--action-policy.pdf
([174]) Mais particularmente, o ICO pode emitir uma notificação de sanção por incumprimento do disposto na *section 149(2)*, *(3)*, *(4)* ou *(5)* do DPA 2018.

responsabilidade do responsável pelo tratamento ou do subcontratante (tendo em conta as medidas técnicas e organizativas aplicadas pelo responsável pelo tratamento ou pelo subcontratante), quaisquer incumprimentos anteriores por parte do responsável pelo tratamento ou do subcontratante, as categorias dos dados pessoais afetadas pelo incumprimento e a circunstância de a sanção ser eficaz, proporcionada e dissuasiva.

(104) O montante máximo da sanção que pode ser imposta por notificação de sanção é de a) 17 500 000 GBP relativamente ao incumprimento dos princípios de proteção dos dados [*sections 35, 36, 37, 38(1), 39(1)* e *40* do DPA 2018], das obrigações de transparência e dos direitos individuais (*sections 44, 45, 46, 47, 48, 49, 52* e *53* do DPA 2018), e dos princípios para as transferências internacionais de dados pessoais (*sections 73, 75, 76, 77* e *78* do DPA 2018); e b) 8 700 000 GBP nos restantes casos ([175]). 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 imposta por uma notificação de sanção é de 17 500 000 GBP.

(105) De acordo com os seus relatórios anuais mais recentes (2018-2019 ([176]), 2019-2020 ([177])), o comissário para a informação realizou um conjunto de investigações relativas ao tratamento de dados pessoais pelas autoridades de aplicação do direito penal. 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 especial centrou-se, em particular, na utilização das capacidades de reconhecimento facial em tempo real pela polícia de Gales do Sul e pelo *Metropolitan Police Service* (MPS). Para além disso, o comissário investigou a «matriz dos gangues» do MPS ([178]) e descobriu um conjunto de violações graves da legislação em matéria de proteção de dados que poderiam reduzir a confiança do público na matriz e na utilização dos dados.

(106) 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.

(107) Outro exemplo de uma ação de execução recente é a coima de 325 000 GBP imposta pelo comissário em maio de 2018 ao *Crown Prosecution Service*, por ter perdido DVD não encriptados que continham gravações de inquéritos policiais. Além disso, o comissário para a informação realizou investigações em 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.

(108) Para além dos poderes sancionatórios do comissário para a informação, determinadas violações da legislação em matéria de proteção de dados constituem infrações e, como tal, podem estar sujeitas a sanções penais (*section 196* do DPA 2018). Tal aplica-se, por exemplo, à obtenção ou divulgação de dados pessoais sem o consentimento do responsável pelo tratamento e à facilitação da divulgação de dados pessoais a outra pessoa sem o consentimento do responsável pelo tratamento ([179]); à reidentificação de informações que são dados pessoais anonimizados sem o consentimento do responsável pelo tratamento que ficou incumbido da anonimização dos dados pessoais ([180]); 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 ([181]), às declarações falsas em resposta a uma notificação informativa ou à destruição de informações relacionadas com notificações informativas e de avaliação ([182]).

(109) O comissário para a informação tem também o dever, por força da *section 139* do DPA 2018, de apresentar às câmaras do parlamento um relatório geral sobre o desempenho das funções que assume no âmbito da referida lei ([183]).

([175]) *Section 157* do DPA 2018.

([176]) *Information Commissioner's Annual Report and Financial Statements 2018-2019* (Relatório anual e demonstrações financeiras do comissário para a informação), disponível na seguinte ligação: https://ico.org.uk/media/about-the-ico/documents/2615262/annual-report-201819.pdf

([177]) *Information Commissioner's Annual Report and Financial Statements 2019-2020* (ver nota de rodapé 157).

([178]) Uma base de dados que registava informações relacionadas com alegados membros de gangues e vítimas da criminalidade de gangues.

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

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

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

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

([183]) Conforme estabelecido no Acordo de Gestão, o relatório anual tem de: i) abranger todas as atividades internas, subsidiárias e conjuntas sob o controlo do ICO; ii) respeitar o *Treasury's Financial Reporting Manual* (Manual para o relato financeiro do tesouro público) (FReM); iii) conter uma declaração sobre a governação, que descreve de que modo o tesoureiro geriu e controlou o recursos utilizados na organização no decurso do ano, demonstrando em que medida a organização procede a uma boa gestão dos riscos na consecução das suas metas e dos seus objetivos; e iv) descrever de modo geral as principais atividades e o desempenho durante o exercício anterior e resumir os planos futuros (Acordo de Gestão para 2018-2021, ponto 3.26, ver nota de rodapé 158).

2.5.2. *Supervisão do sistema judiciário*

(110) A supervisão do tratamento de dados pessoais pelos tribunais e pelo sistema judiciário tem dois objetivos. Caso o titular de um cargo judicial ou um tribunal não atue no exercício de uma competência judicial, o comissário para a informação encarrega-se da supervisão. Caso o responsável pelo tratamento atue no exercício de uma competência judicial ([184]), o ICO não pode exercer as suas funções de supervisão, sendo a supervisão realizada por organismos especiais. Tal reflete a abordagem adotada no artigo 32.º da Diretiva (UE) 2016/680.

(111) 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 *Judicial Data Protection Panel* (Painel de Proteção dos Dados Judiciais) ([185]). Além disso, o presidente do sistema judiciário (*Lord Chief Justice*) e o presidente dos tribunais (*Senior President of Tribunals*) emitiram uma notificação de privacidade ([186]) 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 ([187]) e da Escócia ([188]) emitiram uma notificação semelhante.

(112) 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 (DSJ) ([189]). Também emitiu 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 os problemas decorrentes dessa perda ([190]).

(113) Na Escócia, o Lorde Presidente (*Lord President*) nomeou um juiz supervisor de dados para investigar as reclamações associadas a violações da proteção de dados. Tal encontra-se enunciado nas regras em matéria de reclamações judiciais, que refletem as regras estabelecidas para a Inglaterra e o País de Gales ([191]).

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

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

([185]) O painel é responsável por fornecer orientações e formação ao sistema judiciário. 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 competência judicial. O painel visa proporcionar os meios necessários para a resolução de qualquer 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 não imponha sanções financeiras, caso considere que existe uma violação suficientemente grave do DPA 2018, o painel poderá encaminhar a reclamação para o *Judicial Conduct Investigation Office* (Serviço de Inquérito à Conduta Judicial) (JCIO), que investigará a reclamação. Caso a reclamação seja aceite, cabe ao Lorde Chanceler (*Lord Chancellor*) e ao presidente do sistema judiciário (ou a um alto magistrado para atuar em seu nome) decidir que medida deverá ser tomada contra o titular do cargo judicial. As medidas poderão ser, por ordem de gravidade: recomendação 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, as pessoas singulares podem efetuar nova reclamação junto do *Judicial Appointments and Conduct Ombudsman* (Provedor para as Nomeações e a Conduta Judicial) (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 decorrentes de má administração.

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

([187]) 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

([188]) 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

([189]) O DSJ emite orientações dirigidas ao sistema judiciário e investiga violações e/ou reclamações relativas ao tratamento de dados pessoais efetuado pelos tribunais ou por pessoas singulares no exercício da sua competência judicial.

([190]) Se for considerada grave, a reclamação ou a violação é encaminhada para o *Judicial Complaints Officer* (responsável pelas reclamações judiciais) para novas averiguações, de acordo com o código de boas práticas aplicável às reclamações do presidente do sistema judiciário da Irlanda do Norte. O resultado dessa reclamação pode incluir: a não imposição de medidas adicionais, o aconselhamento, a formação ou mentoria, a advertência informal, a advertência formal, a advertência final, a restrição da prática ou o encaminhamento para um tribunal. O código de boas práticas aplicável às reclamações 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

([191]) Todas as reclamações efetuadas são investigadas pelo juiz supervisor de dados e encaminhadas para o Lorde Presidente, 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).

2.5.3. *Vias de recurso*

(115) 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.

(116) Em primeiro lugar, o 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 ([192]). Conforme descrito nos considerandos 100 e 109, o comissário para a informação tem o poder de avaliar a conformidade com o DPA 2018 do responsável pelo tratamento e do subcontratante, de exigir que estes tomem as medidas necessárias ou se abstenham de tomar medidas em caso de incumprimento e de impor coimas.

(117) Em segundo lugar, o DPA 2018 prevê o direito à ação judicial contra o comissário para a informação. Caso o comissário não «dê seguimento» ([193]) 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 ([194]) para ordenar que o comissário tome as medidas adequadas para dar resposta à reclamação ou informar o autor da reclamação do progresso da reclamação ([195]). Além disso, qualquer pessoa que receba uma das notificações referidas acima (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 poder de apreciação de outra forma, o tribunal tem de permitir o recurso ou substituir por outra notificação ou decisão que poderia ter sido emitida ou proferida pelo comissário para a informação ([196]).

(118) Em terceiro lugar, as pessoas singulares podem intentar uma ação judicial contra um responsável pelo tratamento ou um subcontratante diretamente nos tribunais, ao abrigo 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 ou se abstenha de tomar as medidas especificadas na ordem, no que diz respeito ao tratamento. Além disso, ao abrigo da *section 169* do DPA 2018, qualquer pessoa que tenha sofrido danos por 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 uma 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.

(119) Em quarto lugar, se considerar que houve uma violação dos seus direitos, incluindo do direito à privacidade e à proteção dos dados, por parte das autoridades públicas, qualquer pessoa pode obter reparação junto dos tribunais do Reino Unido ao abrigo do *Human Rights Act 1998*. Os responsáveis pelo tratamento ao abrigo da parte 3 do DPA 2018, ou seja, as autoridades competentes, são sempre autoridades públicas na aceção do *Human Rights Act 1998*. 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 aos direitos em causa em qualquer processo judicial, sempre que essa pessoa seja (ou venha a ser) vítima de um ato ilícito ([197]).

([192]) *Section 165* do DPA 2018.

([193]) 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 seguimento ou do resultado da reclamação antes do fim do prazo de três meses, que tem início quando o comissário recebe 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.

([194]) O tribunal de primeira instância é o tribunal competente para deliberar sobre recursos interpostos 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 competência em todo o Reino Unido.

([195]) *Section 166* do DPA 2018.

([196]) *Sections 161* e *162* do DPA 2018.

([197]) Ver processo Brown/Commissioner of the Met 2016, no qual o tribunal decidiu a favor da parte requerente no contexto da proteção de dados numa ação interposta contra a polícia. O tribunal decidiu a favor da parte requerente, sustentando as suas alegações de violação das obrigações do DPA 1998, de violação do HRA 1998 (e o direito conexo constante do artigo 8.º da CEDH) e de delito de utilização abusiva de informações privadas (a parte requerida admitiu, finalmente, a violação do DPA e da CEDH, pelo que o julgamento se centrou na forma de reparação mais adequada). Em resultado destas violações, o tribunal conferiu uma indemnização pecuniária ao requerente.

(120) Se considerar que algum ato de uma autoridade pública é ilícito, o tribunal pode conferir essa reparação, ou proferir essa decisão, dentro das suas competências e de uma forma que considere justa e adequada ([198]). O tribunal pode igualmente declarar que uma das disposições do direito primário é incompatível com um direito garantido abrigo da CEDH.

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

2.6. **Transferências subsequentes**

(122) O direito do Reino Unido permite a partilha de dados por uma autoridade de aplicação da lei com outras autoridades britânicas para finalidades diferentes daquelas para as quais foram inicialmente recolhidos (denominada «transferência subsequente»), sob reserva de determinadas condições.

(123) 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 inicial 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 para a outra finalidade e o tratamento seja necessário e proporcionado ([199]). Neste caso, todas as garantias previstas na parte 3 do DPA 2018 e analisadas acima são aplicáveis ao tratamento efetuado pela autoridade que os recebe.

(124) Na ordem jurídica do Reino Unido, existem diversas leis que permitem explicitamente a transferência subsequente. Mais particularmente, 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 implique uma perda ou risco de perda para as autoridades públicas ([200]) ou em caso de dívida com uma autoridade pública ou a Coroa ([201]); ii) o *Crime and Courts Act 2013* permite a partilha de informações com a *National Crime Agency* (NCA) ([202]) para o combate, a investigação e a repressão da criminalidade grave e organizada; o *Serious Crime Act 2007* (Lei de 2007 relativa à Criminalidade Grave) permite que as autoridades públicas divulguem informações às organizações antifraude para efeitos de prevenção da fraude ([203]).

(125) Estas leis determinam explicitamente que a partilha de informações deve cumprir as regras estabelecidas no DPA 2018. Além disso, o *College of Policing* publicou a *Authorised Professional Practice on Information Sharing* (Prática Profissional Autorizada para a partilha de informações) ([204]), para auxiliar a polícia no cumprimento das suas obrigações de proteção dos dados previstas no RGPD do Reino Unido, no DPA e no *Human Rights Act 1998*. A conformidade da partilha com o quadro jurídico aplicável para a proteção de dados está, obviamente, sujeita à fiscalização jurisdicional ([205]).

(126) 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 ([206]). Este tipo de partilha abrange dois cenários: 1) quando a autoridade de aplicação do direito penal partilha dados com uma autoridade que não é uma autoridade de aplicação do direito penal nem é uma agência de informações (como, por exemplo, uma autoridade fiscal ou financeira, uma autoridade da concorrência, um serviço de assistência social à infância); 2) quando uma autoridade

([198]) *Section 8(1)* do *Human Rights Act 1998*.
([199]) *Section 36(3)* do DPA 2018.
([200]) *Section 56* do *Digital Economy Act 2017*, disponível na seguinte ligação https://www.legislation.gov.uk/ukpga/2017/30/contents
([201]) *Section 48* do *Digital Economy Act 2017*.
([202]) *Section 7* do *Crime and Courts Act 2013*, disponível na seguinte ligação: https://www.legislation.gov.uk/ukpga/2013/22/contents
([203]) *Section 68* do *Serious Crime Act 2007*, disponível na seguinte ligação https://www.legislation.gov.uk/ukpga/2007/27/contents
([204]) *Authorised Professional Practice on Information Sharing*, disponível na seguinte ligação: https://www.app.college.police.uk/app-content/information-management/sharing-police-information
([205]) Ver, por exemplo, o processo M/the Chief Constable of Sussex Police [2019] EWHC 975 (Admin), no qual foi pedido ao *High Court* que analisasse a partilha de dados entre a polícia e a *Business Crime Reduction Partnership* (BCRP), uma organização habilitada a gerir regimes de notificações de exclusão, que proíbem as pessoas de entrar nas instalações comerciais dos seus membros. O tribunal analisou a partilha de dados, que decorria com base num acordo que tinha como finalidade proteger o público e prevenir a criminalidade e, por fim, concluiu que a maioria dos aspetos da partilha de dados era lícita, à exceção de algumas informações sensíveis partilhadas entre a polícia e a 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.
([206]) *Section 36(4)* do DPA 2018.

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. Conforme referido na Decisão adotada ao abrigo do Regulamento (UE) 2016/679, as garantias previstas pelo RGPD do Reino Unido e a parte 2 do DPA 2018 prestam um nível de proteção que é essencialmente equivalente ao prestado na União ([207]).

(127) No segundo cenário, no que diz respeito à partilha de dados recolhidos por uma autoridade de aplicação do direito penal com uma agência de informações para efeitos de segurança nacional, a base jurídica que autoriza essa partilha é o *Counter Terrorism Act 2008* (Lei de 2008 relativa ao Combate ao Terrorismo) (CTA 2008) ([208]). Ao abrigo da CTA 2008, qualquer pessoa pode facultar informações a quaisquer serviços de informações para efeitos de cumprimento das funções desse serviço, incluindo as funções de «segurança nacional».

(128) No que diz respeito às condições em que os dados podem ser partilhados para efeitos de segurança nacional, o *Intelligence Service Act* (Lei relativa ao Serviço de Informações) e o *Security Service Act* (Lei relativa ao Serviço de Segurança) limitam a capacidade de obtenção dos dados dos serviços de informações aos dados estritamente necessários ao desempenho das suas funções legais. As autoridades competentes, abrangidas pelo âmbito de aplicação da parte 3 do DPA 2018, que procuram partilhar dados com os serviços de informações terão de ter em consideração um conjunto de fatores/limitações, para além das funções legais das agências que são criadas no *Intelligence Service Act* e no *Security Service Act* ([209]). A *section 20* do CTA 2008 clarifica que qualquer partilha de dados efetuada nos termos da *section 19* do CTA 2008 tem de cumprir, ainda assim, a legislação em matéria de proteção de dados; o que significa que todas as limitações e requisitos do DPA 2018 são aplicáveis. Além disso, as autoridades de aplicação da lei e os serviços de informações são autoridades públicas para efeitos do *Human Rights Act 1998*, tendo, por conseguinte, de assegurar que atuam em conformidade com os direitos garantidos ao abrigo da CEDH, incluindo o respetivo artigo 8.º. Por outras palavras, estes requisitos significam que qualquer partilha de dados entre as agências de aplicação da lei e os serviços de informações tem de cumprir a legislação em matéria de proteção de dados e a CEDH.

(129) O tratamento, por parte dos serviços de informações, de dados pessoais recebidos ou obtidos a partir de autoridades de aplicação da lei para finalidades de segurança nacional está sujeito a um conjunto de condições e garantias ([210]). A parte 4 do DPA 2018 é aplicável a todo o tratamento efetuado pelos serviços de informações ou

([207]) Decisão de Execução da Comissão nos termos do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho sobre a adequação do nível de proteção dos dados pessoais assegurado pelo Reino Unido [C(2021) 4800].

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

([209]) A *section 2(2)* do *Intelligence Service Act 1994* (ver https://www.legislation.gov.uk/ukpga/1994/13/contents) determina que «[o] responsável do serviço de informações é responsável pela eficácia desse 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 — i) para o 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 promover os interesses de algum partido político do Reino Unido», ao passo que a *section 2(2)* do *Security Service Act 1989* (ver https://www.legislation.gov.uk/ukpga/1989/5/contents) 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 apenas obtém as informações estritamente necessárias ao exercício adequado das suas funções e que 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]; b) que o serviço não toma nenhuma medida para promover 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».

([210]) As salvaguardas e as limitações dos poderes dos serviços de informações também são regulamentadas pelo *Investigatory Powers Act 2016*, que, juntamente com o *Regulation of Investigatory Powers Act 2000* (Regulamento de 2000 relativo aos poderes de investigação), para a Inglaterra, o País de Gales e a Irlanda do Norte, e o *Regulation of Investigatory Powers (Scotland) Act 2000* [Regulamento de 2000 (da Escócia) relativo aos poderes de investigação], para a Escócia, proporcionam a base jurídica para a utilização de tais poderes. No entanto, estes poderes não são pertinentes no contexto da «transferência subsequente», uma vez que abrangem a recolha direta de dados pessoais por parte das agências de informações. Para uma avaliação dos poderes concedidos às agências de informações ao abrigo do *Investigatory Powers Act*, ver a Decisão de Execução da Comissão nos termos do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho sobre a adequação do nível de proteção dos dados pessoais assegurado pelo Reino Unido [C (2021) 4800].

em seu nome. Estabelece os principais princípios de proteção de dados (licitude, lealdade e transparência ([211]); limitação das finalidades ([212]); minimização dos dados ([213]); exatidão ([214]); limitação da conservação ([215]) e segurança ([216]), impõe condições para o tratamento de categorias especiais de dados ([217]), prevê os direitos dos titulares dos dados ([218]), exige a proteção de dados desde a conceção ([219]) e regulamenta as transferências internacionais de dados pessoais ([220]).

(130) Paralelamente, a *section 110* do DPA 2018 prevê uma isenção de determinadas disposições na parte 4 do DPA 2018 quando essa isenção é necessária para proteger a segurança nacional. 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, determinados poderes sancionatórios do comissário para a informação, as disposições que criminalizam determinadas violações da proteção de dados e as disposições relativas às finalidades de tratamento especiais, como os fins jornalísticos, académicos ou artísticos. É possível recorrer a esta isenção com base numa análise caso a caso ([221]). Conforme explicado pelas autoridades do Reino Unido e confirmado pela jurisprudência do Reino Unido, «(um) responsável pelo tratamento tem de 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» ([222]). Cabe à supervisão do ICO determinar se a isenção foi usada adequadamente ou não ([223]).

([211]) Ao abrigo da *section 86(6)* do DPA 2018, para determinar a lealdade e a transparência do tratamento, há que ter em consideração o método empregue para a obtenção dos dados. Neste sentido, o requisito de lealdade e transparência é preenchido se os dados forem obtidos junto de uma pessoa que esteja legalmente autorizada ou obrigada a fornecê-los.

([212]) Ao abrigo da *section 87* do DPA 2018, as finalidades do tratamento têm de ser determinadas, explícitas e legítimas. Os dados não podem ser tratados de uma forma incompatível com as finalidades para as quais foram recolhidos. Ao abrigo da *section 87(3)* 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 proporcionado para essa outra finalidade. As operações de tratamento devem ser consideradas tratamento compatível se se compuserem de operações de tratamento para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos e estiverem sujeitas a garantias adequadas [*section 87(4)* do DPA 2018].

([213]) Os dados pessoais têm de ser adequados, relevantes e não excessivos (*section 88* do DPA 2018).

([214]) Os dados pessoais têm de ser precisos e atualizados (*section 89* do DPA 2018).

([215]) Os dados pessoais têm de ser conservados apenas durante o período necessário (*section 90* do DPA 2018).

([216]) O sexto princípio de proteção de dados consiste na obrigatoriedade de os dados pessoais serem 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 (nomeadamente) o 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 tendo em conta 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.

([217]) *Section 86(2)(b)* e *schedule 10* do DPA 2018.

([218]) 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 automatizada, de intervir na decisão automatizada e de ser informado da decisão automatizada. Além disso, o responsável pelo tratamento tem de informar o titular dos dados do tratamento dos seus dados pessoais.

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

([220]) *Section 109* do DPA 2018. É possível efetuar transferências de dados pessoais para organizações internacionais ou países fora do Reino Unido caso as transferências constituam uma medida necessária e proporcionada para efeitos das funções legais do responsável pelo tratamento ou para outras finalidades previstas em artigos específicos do *Security Service Act 1989* e do *Intelligence Service Act 1994*.

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

([222]) *UK Explanatory Framework for Adequacy Discussions, Section H: National Security Data Protection and Investigatory Powers Framework* (Quadro explicativo do Reino Unido para as conversações em matéria de adequação, secção H: Proteção dos dados no âmbito da segurança nacional e quadro dos poderes de investigação), p 15 e 16, disponível na seguinte ligação: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872239/H_-_National_Security.pdf. Ver igualmente processo *Baker/Secretary of State* (ver nota de rodapé 220 acima), no qual o tribunal anulou um certificado de segurança nacional emitido pelo ministro da tutela e 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, ao permitir essa isenção em todas as circunstâncias sem uma análise caso a caso, excedeu-se o que seria necessário e proporcionado para a proteção da segurança nacional.

([223]) Ver o memorando de entendimento entre o ICO e a comunidade de serviços de informações do Reino Unido, 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, de que a aplicação de eventuais isenções foi utilizada adequadamente» (memorando de entendimento entre o Gabinete do Comissário para a Informação e a comunidade de 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).

(131) Além disso, no que se refere à possibilidade de restringir a aplicação de qualquer um dos direitos mencionados acima para efeitos de proteção da «segurança nacional», a *section 79* do DPA 2018 prevê a possibilidade de um responsável pelo tratamento 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 ([224]). O Governo do Reino Unido emitiu uma orientação sobre o certificado de segurança nacional ao abrigo do DPA 2018 que, nomeadamente, salienta que qualquer limitação dos direitos dos titulares dos dados para efeitos de proteção da segurança nacional tem de ser necessária e proporcionada ([225]). Todos os certificados de segurança nacional têm de ser publicados no sítio Web do ICO ([226]).

(132) O certificado deve ter uma duração fixa não superior a cinco anos, para que seja analisado regularmente pelo poder executivo ([227]). O certificado tem de 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 ([228]).

(133) 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. Ou seja, o responsável pelo tratamento ou o subcontratante só pode recorrer a um certificado quando tiver a certeza de que é necessário recorrer à isenção por motivos de segurança nacional, que tem de ser aplicada caso a caso. 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 ([229]).

(134) As pessoas diretamente afetadas pela emissão do certificado podem recorrer ao *Upper Tribunal* ([230]) para contestar o certificado ([231]) ou, caso o certificado inclua a identificação dos dados por meio de uma descrição geral, para contestar a aplicação do mesmo a dados específicos ([232]).

(135) O tribunal analisará a decisão de emitir um certificado e decidirá se existiram motivos razoáveis para a emissão do certificado ([233]). 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 considerando 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 ([234]).

([224]) O DPA 2018 revogou a possibilidade de emitir certificados ao abrigo da *section 28(2)* do *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 afigura-se 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 observar 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. De momento não foram emitidos nenhuns certificados de segurança nacional ao abrigo do DPE 1998.

([225]) *United Kingdom Government Guidance on National Security Certificates under the Data Protection Act 2018* (orientação 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

([226]) 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 divulgará, todavia, o facto de o certificado ter sido emitido.

([227]) *United Kingdom Government Guidance on National Security Certificates*, ponto 15, ver nota de rodapé 225.

([228]) *United Kingdom Government Guidance on National Security Certificates*, ponto 5, ver nota de rodapé 225.

([229]) A *section 102* do DPA 2018 exige que o responsável pelo tratamento demonstre que cumpriu o DPA 2018. Tal implica que o serviço de informações teria 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, disponível na seguinte ligação: https://ico.org.uk/about-the-ico/ /our-information/national-security-certificates/

([230]) 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.

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

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

([233]) No processo *Baker/Secretary of State* (ver nota de rodapé 221), o *Information Tribunal* (tribunal especializado em questões de informação) anulou um certificado de segurança nacional emitido pelo ministro da tutela, tendo em conta que não havia motivo para criar uma exceção geral da obrigação de responder a pedidos de acesso e que, ao permitir essa exceção em todas as circunstâncias sem uma análise caso a caso, excedeu-se o que seria necessário e proporcionado para a proteção da segurança nacional.

([234]) *United Kingdom Government Guidance on National Security Certificates*, ponto 25, ver nota de rodapé 224.

(136) 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 ([235]) para salvaguardar outros importantes objetivos de interesse público geral ou interesses protegidos, como, por exemplo, o privilégio parlamentar, a prerrogativa legal de confidencialidade, a conduta dos processos judiciais ou a eficácia do combate das forças armadas. A aplicação destas disposições é dispensada para determinadas categorias de dados («com base na categoria») ou é dispensada na medida em que a aplicação destas disposições seria suscetível de prejudicar o interesse protegido («com base no prejuízo») ([236]). As isenções com base no prejuízo só podem ser invocadas na medida em que a aplicação da disposição de proteção de dados enunciada fosse suscetível de prejudicar o interesse específico em questão. Por conseguinte, a utilização de uma isenção tem de ser sempre justificada referindo o prejuízo relevante que seria suscetível de ocorrer no caso individual. As isenções com base na categoria só podem ser invocadas relativamente à categoria de dados específica e definida de modo circunscrito para a qual é concedida a isenção. A sua finalidade e o seu efeito são semelhantes a diversas exceções previstas no RGPD do Reino Unido (no *schedule* 2 do DPA 2018), que, por sua vez, refletem as previstas no artigo 23.º do RGPD.

(137) Resulta do que precede que estão previstas limitações e condições ao abrigo das disposições legais aplicáveis do Reino Unido, conforme igualmente interpretado pelos tribunais e pelo comissário para a informação, para garantir que essas isenções e limitações permanecem dentro dos limites do necessário e proporcionado para proteger a segurança nacional.

(138) O tratamento de dados pessoais realizado pelos serviços de informações ao abrigo da parte 4 do DPA 2018 é supervisionado pelo comissário para a informação ([237]).

(139) 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 suas obrigações, a prestação de informações aos titulares dos dados relativamente ao exercício dos seus direitos e a realização de investigações.

(140) 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 emitir advertências na eventualidade de uma operação de tratamento ser suscetível de 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 ([238]). No entanto, contrastando com outras partes do DPA 2018, o comissário não pode emitir uma notificação de avaliação a um organismo de segurança nacional ([239]).

(141) Além disso, a *section 110* do DPA 2018 prevê uma exceção à utilização de determinados poderes do comissário sempre que necessário por motivos 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) e o poder de realizar inspeções em conformidade com as obrigações internacionais, os poderes

([235]) Estas incluem: 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 de dados; e iii) os deveres relativos à denúncia de violações ao ICO.

([236]) De acordo com o quadro explicativo do Reino Unido, as isenções «baseadas na categoria» são: i) informações sobre a concessão de títulos e altos cargos da Coroa; ii) a prerrogativa legal de confidencialidade; iii) referências confidenciais em matéria de emprego, formação ou educação; e iv) as respostas e classificações 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. *UK Explanatory Framework for Adequacy Discussions, Section H: National Security*, p. 13, ver nota de rodapé 222.

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

([238]) Nos termos da *section 149(2)* do DPA 2018, lida em conjugação com a *section 155*, as notificações de execução e sanção podem ser emitidas a um responsável pelo tratamento ou a um subcontratante relativamente a violações da parte 4, capítulo 2, do DPA 2018 (princípios do tratamento), uma disposição da parte 4 do DPA 2018 que confere direitos a um titular de dados, um requisito de comunicação de uma violação de dados pessoais ao comissário imposto pela *section 108* do DPA 2018 e os princípios aplicáveis às transferências de dados pessoais para países terceiros, países que não sejam signatários da convenção e organizações internacionais da *section 109* do DPA 2018. (Para mais informações sobre a notificação de execução e sanção, ver os considerandos 102)a 103).

([239]) Nos termos da *section 147(6)* do DPA 2018, o comissário para a informação não pode remeter uma notificação de avaliação a um organismo indicado na *section 23(3)* do *Freedom of Information Act 2000* (Lei de 2000 relativa à liberdade de informação). Entre eles incluem-se o *Security Service* (MI5), o *Secret Intelligence Service* (MI6) e o quartel-general de comunicações do governo.

de entrada e inspeção e as normas em matérias de infrações ([240]). Como explicado no considerando 136, estas exceções aplicar-se-ão apenas se necessário e proporcionado, bem como caso a caso. A aplicação destas exceções pode ser objeto de fiscalização jurisdicional ([241]).

(142) O ICO e os serviços de informações do Reino Unido assinaram um memorando de entendimento ([242]) 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. Mais particularmente, nele prevê-se que, ao receber uma reclamação, o ICO avaliará se foi adequadamente invocada uma isenção de segurança nacional. As respostas às perguntas formuladas pelo ICO no contexto da análise das reclamações individuais têm de ser dadas no prazo de 20 dias úteis de acordo com as orientações do Governo do Reino Unido sobre os certificados de segurança nacional ao abrigo do *Data Protection Act*, por meio dos canais seguros adequados se envolver informações classificadas. Desde abril de 2018 até à data, o ICO recebeu 21 reclamações de pessoas singulares sobre os serviços de informações. Cada reclamação foi avaliada e o resultado foi comunicado ao titular dos dados ([243]).

(143) Além disso, a *Intelligence and Security Committee* (comissão para as informações e a segurança) (ISC) desempenha uma função de supervisão parlamentar em matéria de tratamento de dados pelos serviços de informações. Esta comissão encontra a sua base jurídica no *Justice and Security Act 2013* (Lei de 2013 relativa à justiça e segurança) (JSA 2013) ([244]). A referida lei estabelece a ISC enquanto comissão do parlamento do Reino Unido. A ISC é composta por membros pertencentes a ambas as câmaras do parlamento e nomeados pelo primeiro-ministro na sequência de uma consulta ao líder da oposição ([245]). A ISC está obrigada a apresentar um relatório anual ao parlamento sobre o exercício das respetivas funções, bem como outros relatórios que considere adequados ([246]).

(144) Desde 2013, a ISC tem recebido cada vez mais poderes, incluindo a supervisão das atividades operacionais dos serviços de segurança. Ao abrigo da secção 2 da JSA 2013, a ISC está incumbida de supervisionar as despesas, a administração, as políticas e o funcionamento das agências nacionais de segurança. A JSA 2013 especifica que a ISC

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

([241]) Ver, por exemplo, processo *Baker/Secretary of State for the Home Department* (ver nota de rodapé 221).

([242]) Memorando de entendimento entre o ICO e a comunidade dos serviços de informações do Reino Unido, ver nota de rodapé 231.

([243]) Em sete destes casos, o ICO aconselhou o reclamante a suscitar as suas preocupações junto do responsável pelo tratamento (trata-se dos casos em que a pessoa suscitou as suas preocupações junto do ICO, mas deveria tê-lo feito primeiro junto do responsável pelo tratamento), num dos casos, o ICO aconselhou de modo geral o 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 preocupação fosse suscitada junto do ICO) e noutros 13 casos não foi necessária qualquer medida por parte do responsável pelo tratamento (esta opção é utilizada quando as preocupações suscitadas pelas pessoas são abrangidas pelo *Data Protection Act 2018* uma vez que dizem respeito ao tratamento de informações pessoais, mas, com base nas informações transmitidas, não se afigura que o responsável pelo tratamento tenha violado a legislação).

([244]) Conforme explicado pelas autoridades do Reino Unido, a JSA expandiu 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.

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

([246]) Os relatórios e as declarações da comissão estão disponíveis em linha na seguinte ligação: http://isc.independent.gov.uk/committee-reports. 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://b1cba9b3-a-5e6631fd-s-sites.googlegroups.com/a/independent.gov.uk/isc/files/20150312_ISC_P%2BS%2BRpt%28web%29.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, a 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

pode realizar investigações sobre matérias operacionais quando estas não digam respeito a operações em curso ([247]). O memorando de entendimento celebrado entre o primeiro-ministro e a ISC ([248]) especifica os elementos a ter em conta ao apurar se uma atividade integra ou não uma operação em curso ([249]). O primeiro-ministro também pode solicitar que a ISC investigue operações em curso, podendo esta analisar informações transmitidas voluntariamente pelas agências.

(145) Nos termos do *schedule 1* do JSA 2013, a ISC pode solicitar a divulgação de qualquer informação aos responsáveis por qualquer um dos três serviços de informações. A agência tem de disponibilizar a referida informação, a menos que o ministro da tutela o recuse ([250]). As autoridades do Reino Unido explicaram que, na prática, são retidas muito poucas informações solicitadas pela ISC ([251]).

(146) No que respeita às vias de recurso, em primeiro lugar, ao abrigo da *section 165(2)* do DPA 2018, o titular dos dados pode apresentar reclamação junto do ICO se considerar que existe uma violação de dados pessoais a si respeitantes no âmbito da parte 4 do DPA 2018, incluindo qualquer utilização abusiva das derrogações e limitações de segurança nacional.

(147) 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 ([252]), de oposição ao tratamento ([253]) e de retificação ou apagamento.

(148) 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 ([254]). Os danos incluem perdas financeiras e não financeiras, como sofrimento emocional ([255]).

(149) Por fim, as pessoas podem apresentar reclamação junto do *Investigatory Powers Tribunal* (Tribunal dos Poderes de Investigação) por qualquer ato praticado pelas agências de informações do Reino Unido ou em seu nome ([256]). O *Investigatory Powers Tribunal* (IPT) foi criado pelo *Regulation of Investigatory Powers Act 2000*, para a Inglaterra, o País de Gales e a Irlanda do Norte, e o *Regulation of Investigatory Powers (Scotland) Act 2000* (RIPA 2000), para a Escócia ([257]). Nos termos da *section 65* do RIPA 2000, os membros do IPT são nomeados pela rainha por um período de cinco anos.

(150) Os membros podem ser afastados do seu cargo pela rainha na sequência de um comunicado ([258]) de ambas as câmaras do parlamento ([259]).

(151) Para intentar uma ação junto do IPT («requisito de legitimidade»), nos termos da *section 65* do RIPA 2000, uma pessoa singular tem de estar convicta de que i) os atos de um serviço de informações ocorreram 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 ([260]), e ii) os atos ocorreram

([247]) *Section 2* do JSA 2013.
([248]) 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
([249]) Memorando de entendimento entre o primeiro-ministro e a ISC, ponto 14, ver nota de rodapé 248.
([250]) O ministro da tutela só pode recusar a divulgação da informação por dois motivos: a informação é sensível e não deve ser divulgada à ISC a bem da segurança nacional; ou trata-se de informação de tal natureza que, se fosse chamado a produzi-la perante uma comissão especial parlamentar da Câmara dos Comuns, levaria o ministro da tutela a considerar (por motivos que não se limitam à segurança nacional) que seria conveniente não o fazer (*schedule 1*, n.º 4, ponto 2, da JSA 2013).
([251]) *UK Explanatory Framework – Section H: National Security*, p. 43.
([252]) *Section 94(11)* do DPA 2018.
([253]) *Section 99(4)* do DPA 2018.
([254]) *Section 169* do DPA 2018, que 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 pessoais».
([255]) *Section 169(5)* do DPA 2018.
([256]) Ver *section 65(2)(b)* do RIPA.
([257]) Nos termos do *schedule 3* do RIPA 2000, os membros têm de ter uma determinada experiência judicial e o seu mandato é renovável.
([258]) Sobre a noção de «comunicado», ver nota de rodapé 183.
([259]) *Schedule 3*, n.º 1, ponto 5, do RIPA 2000.
([260]) *Section 65(4)* do RIPA 2000.

em «circunstâncias contestáveis» ([261]) ou «foram praticados pelos serviços de informações ou em nome destes» ([262]). Dado que este paradigma da «convicção», em particular, tem sido interpretado de forma bastante ampla ([263]), o recurso ao tribunal está sujeito a requisitos de legitimidade relativamente baixos.

(152) Quando o referido tribunal considera uma reclamação que lhe foi apresentada, incumbe-lhe o dever de 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 os alegados atos ocorreram ([264]). Quando aprecia um processo, o referido tribunal tem de aplicar os mesmos princípios para proceder à sua determinação que seriam aplicados por um tribunal num pedido de fiscalização jurisdicional ([265]).

(153) O tribunal tem de notificar o autor da reclamação se houve ou não determinação a seu favor ([266]). 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 ([267]). Nos termos da *section 67A* do RIPA 2000, as determinações do tribunal podem ser objeto de recurso, sob reserva de uma autorização do referido tribunal ou do tribunal de recurso competente.

(154) Mais particularmente, as pessoas podem intentar uma ação — e obter reparação — junto do IPT se considerarem que uma autoridade pública atuou (ou pretende atuar) de modo incompatível com os direitos consagrados na CEDH, incluindo o direito à privacidade e proteção de dados, e que é, por conseguinte, ilícito por força da *section 6(1)* do *Human Rights Act 1998*. Foi concedida ao IPT competência exclusiva para todas as reclamações relativas ao *Human Rights Act* relacionadas com as agências de informações. Tal significa, conforme referido pelo *High Court*, que «a questão de ter havido uma violação do HRA relativamente aos factos de um determinado processo 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 próprio IPT está agora sujeito à possibilidade de recurso num tribunal de recurso competente (na Inglaterra e no País de Gales, o *Court of Appeal*); e que o *Supreme Court* decidiu recentemente que o IPT é, em princípio, passível de fiscalização jurisdicional: ver *R (Privacy International)/Investigatory Powers Tribunal* [2019] UKSC 22; [2019] 2 WLR 1219» ([268]). Se considerar que algum ato de uma autoridade pública é ilícito, o IPT pode conferir essa reparação, ou proferir essa decisão, dentro das suas competências e de uma forma que considere justa e adequada ([269]).

([261]) Tais circunstâncias dizem respeito aos atos das autoridades públicas que ocorrem num contexto de autoridade (por exemplo, um mandado, uma autorização/notificação para a aquisição de comunicações, etc.) ou se as circunstâncias forem tais (exista ou não tal autoridade) que não teria sido adequado que os atos tivessem sido praticados sem ela, ou pelo menos sem ter sido dada a devida consideração se tal autoridade deveria ser solicitada. Os atos autorizados por um comissário judicial são considerados como tendo ocorrido em circunstâncias contestáveis [*section 65* (*7ZA*) do RIPA 2000], enquanto outros atos que ocorrem com a autorização de uma pessoa que exerça funções jurisdicionais são considerados como não tendo ocorrido em circunstâncias contestáveis [*section 65(7)* e *(8)* do RIPA 2000].

([262]) De acordo com as informações fornecidas pelas autoridades do Reino Unido, o baixo limiar para a apresentação de uma reclamação implica que não é raro que a investigação do tribunal determine que o autor da reclamação nunca foi, na verdade, objeto de investigação por uma autoridade pública. O último relatório estatístico do IPT 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 utilizadas atividades/poderes encobertos em relação aos autores das reclamações, ou que foram utilizadas técnicas encobertas e que o tribunal determinou que a atividade era lícita. Além disso, 11% foram excluídas da 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

([263]) Ver processo *Human Rights Watch/Secretary of State* [2016] UKIPTrib15_165-CH. Neste processo, o *Investigatory Powers Tribunal*, remetendo para jurisprudência do TEDH, considerou que o critério adequado no que respeita à convicção de que um ato abrangido pela *subsection 68(5)* do RIPA 2000 foi levado a cabo por qualquer um dos serviços de informações ou em seu nome consiste em apurar 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 de 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).

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

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

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

([267]) Tal pode incluir uma ordem que exija a destruição de qualquer gravação de informações detida por qualquer autoridade pública relacionada com qualquer pessoa.

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

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

(155) Depois de esgotarem as vias de recurso nacionais, as pessoas singulares podem recorrer ao Tribunal Europeu dos Direitos Humanos por violações dos direitos garantidos pela CEDH, incluindo o direito à privacidade e à proteção de dados.

(156) Do que precede, resulta que a partilha, por pate de autoridades de aplicação do direito penal do Reino Unido, de dados transferidos ao abrigo da presente decisão com outras autoridades públicas, incluindo agências de informações, é enquadrada por limitações e condições que asseguram que tais transferências subsequentes são necessárias e proporcionadas e estão sujeitas a garantias em matéria de proteção de dados específicas ao abrigo do DPA 2018. Além disso, o tratamento de dados pelas autoridades públicas em causa é supervisionado por organismos independentes, tendo as pessoas afetadas acesso a vias de recurso judicial eficazes.

3. **CONCLUSÃO**

(157) A Comissão entende que a parte 3 do DPA 2018 assegura um nível de proteção dos dados pessoais transferidos para efeitos de aplicação do direito penal das autoridades competentes da União para as autoridades competentes do Reino Unido que é essencialmente equivalente ao garantido pela Diretiva (UE) 2016/680.

(158) Além disso, a Comissão considera que os mecanismos de controlo e as vias de recurso previstas 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 o apagamento dos mesmos.

(159) Por último, com base nas informações disponíveis sobre o quadro jurídico do Reino Unido, a Comissão entende que qualquer ingerência nos direitos fundamentais das pessoas singulares, cujos dados pessoais sejam transferidos da União Europeia para o Reino Unido pelas autoridades públicas do Reino Unido para fins de interesse público, incluindo no contexto da partilha de dados pessoais entre autoridades de aplicação da lei e outras autoridades públicas como organismos de segurança nacional, será limitada ao estritamente necessário para alcançar o objetivo legítimo em causa, existindo uma proteção jurídica eficaz contra tal ingerência.

(160) Assim, há que decidir que o Reino Unido garante um nível adequado de proteção na aceção do artigo 36.º, n.º 2, da Diretiva (UE) 2016/680, interpretado à luz da Carta dos Direitos Fundamentais da União Europeia.

(161) Esta conclusão baseia-se tanto no regime interno britânico relevante 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.

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

(162) Os Estados-Membros e os respetivos órgãos são obrigados a tomar as medidas necessárias para cumprir os atos das instituições da União, uma vez que se presume que estes últimos 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.

(163) Consequentemente, uma decisão de adequação da Comissão adotada nos termos do artigo 36.º, n.º 3, da Diretiva (UE) 2016/680 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 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.

(164) Ao mesmo tempo, importa recordar que, em conformidade com o artigo 47.º, n.º 5, da Diretiva (UE) 2016/680, e conforme explicado pelo Tribunal de Justiça no acórdão proferido no processo Schrems, quando uma autoridade nacional responsável pela proteção de dados, incluindo na sequência de uma reclamação, questiona a compatibilidade de uma decisão de adequação da Comissão com os direitos fundamentais à privacidade e à proteção dos dados da pessoa singular, o direito nacional tem de prever vias de recurso que lhe permitam invocar as críticas junto de um tribunal nacional, que poderá ter de proceder a um reenvio prejudicial para o Tribunal de Justiça ([270]).

([270]) *Schrems*, n.º 65.

5. CONTROLO, SUSPENSÃO, REVOGAÇÃO OU ALTERAÇÃO DA PRESENTE DECISÃO

(165) Nos termos do artigo 36.º, n.º 4, da Diretiva (UE) 2016/680, a Comissão tem de controlar, de forma continuada, os desenvolvimentos pertinentes no Reino Unido após a adoção da presente decisão, a fim de avaliar se 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, que pode ser suscetível de evoluir. A este respeito, prestar-se-á especial atenção à aplicação, na prática, das regras do Reino Unido em matéria de transferências de dados pessoais para países terceiros, nomeadamente por meio da celebração de acordos internacionais, e ao impacto que podem ter no nível de proteção oferecido aos dados transferidos ao abrigo da presente decisão, bem como à eficácia do exercício dos direitos das pessoas nos domínios abrangidos pela presente decisão. Entre outros elementos, o controlo da Comissão basear-se-á nos desenvolvimentos da jurisprudência e na supervisão do ICO e de outros organismos independentes.

(166) A fim de facilitar este controlo, as autoridades do Reino Unido devem informar pronta e regularmente a Comissão de qualquer alteração significativa do ordenamento jurídico britânico que tenha impacto no quadro jurídico objeto da presente decisão, bem como de qualquer evolução nas práticas relacionadas com o tratamento dos dados pessoais avaliadas na presente decisão, nomeadamente no respeitante aos elementos referidos no considerando 165.

(167) 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 para autoridades competentes no Reino Unido. A Comissão deve igualmente ser informada sobre quaisquer indícios de que as ações das autoridades públicas britânicas responsáveis pela prevenção, investigação, deteção ou repressão de infrações penais, incluindo os organismos de controlo, não asseguram o nível de proteção exigido.

(168) 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 razoável a especificar, que não pode exceder três meses. Se necessário, este prazo pode ser prorrogado por um período determinado, tendo em conta a natureza da questão em causa e/ou das medidas a adotar.

(169) Se, uma vez decorrido o prazo especificado, as autoridades britânicas competentes 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 58.º, n.º 2, da Diretiva (UE) 2016/680 com vista à suspensão total ou parcial ou à revogação da presente decisão.

(170) 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.

(171) Por imperativos de urgência devidamente justificados, a Comissão recorrerá à possibilidade de adotar, em conformidade com o procedimento referido no artigo 58.º, n.º 3, da Diretiva (UE) 2016/680, atos de execução imediatamente aplicáveis que suspendam, revoguem ou alterem a decisão.

6. VIGÊNCIA E RENOVAÇÃO DA PRESENTE DECISÃO

(172) Há que 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 União Europeia. Tal pode envolver, nomeadamente, alterações ou modificações do quadro de proteção de dados avaliado na presente decisão, bem como outros desenvolvimentos pertinentes.

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

(174) 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, ampliando o seu âmbito de aplicação temporal, 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 58.º, n.º 2, do Regulamento (UE) 2016/680.

7. **CONSIDERAÇÕES FINAIS**

(175) O Comité Europeu para a Proteção de Dados publicou o seu parecer ([271]), que foi tido em conta na elaboração da presente decisão.

(176) As medidas previstas na presente decisão estão em conformidade com o parecer do comité criado ao abrigo do artigo 58.º da Diretiva (UE) 2016/680.

(177) Nos termos do artigo 6.º-A do Protocolo n.º 21 relativo à posição do Reino Unido e da Irlanda em relação ao espaço de liberdade, segurança e justiça, anexo ao TUE e ao TFUE, a Irlanda não fica vinculada pelas regras estabelecidas na Diretiva (UE) 2016/680, e, por conseguinte, pela presente decisão de execução, que digam respeito ao tratamento de dados pessoais pelos Estados-Membros no exercício de atividades relativas à aplicação da parte III, título V, capítulo 4 ou 5, do TFUE, caso a Irlanda não esteja vinculada por regras que regem as formas de cooperação judiciária em matéria penal ou de cooperação policial no âmbito das quais devem ser observadas as disposições definidas com base no artigo 16.º do TFUE. Além disso, em virtude da Decisão de Execução (UE) 2020/1745 do Conselho ([272]), a Diretiva (UE) 2016/680 entra em vigor e é aplicada a título provisório na Irlanda a partir de 1 de janeiro de 2021. Por conseguinte, a Irlanda fica vinculada pela presente decisão de execução, nas condições previstas para a aplicação da Diretiva (UE) 2016/680 na Irlanda em conformidade com a Decisão de Execução (UE) 2020/1745, no que respeita ao acervo de Schengen em que participa.

(178) Nos termos dos artigos 2.º e 2.º-A do Protocolo n.º 22 relativo à posição da Dinamarca, anexo ao Tratado da União Europeia e ao Tratado sobre o Funcionamento da União Europeia, a Dinamarca não fica vinculada nem sujeita à aplicação das regras estabelecidas na Diretiva (UE) 2016/680, e, por conseguinte, à presente decisão de execução, que digam respeito ao tratamento de dados pessoais pelos Estados-Membros no exercício de atividades abrangidas pelo âmbito de aplicação da parte III, título V, capítulo 4 ou 5, do TFUE. Contudo, uma vez que a Diretiva (UE) 2016/680 se baseia no acervo de Schengen, a Dinamarca, em conformidade com artigo 4.º do referido protocolo, notificou, em 26 de outubro de 2016, a sua decisão de transpor a Diretiva (UE) 2016/680. Por conseguinte, a Dinamarca fica vinculada, por força do direito internacional, a dar execução à presente decisão de execução.

(179) No que diz respeito à Islândia e à Noruega, a presente decisão de execução constitui um desenvolvimento das disposições do acervo de Schengen, na aceção do acordo celebrado entre o Conselho da União Europeia e a Islândia e o Reino da Noruega relativo à associação destes Estados à execução, à aplicação e ao desenvolvimento do acervo de Schengen ([273]).

(180) No que diz respeito à Suíça, a presente decisão de execução constitui um desenvolvimento das disposições do acervo de Schengen, na aceção do Acordo entre a União Europeia, a Comunidade Europeia e a Confederação Suíça relativo à associação da Confederação Suíça à execução, à aplicação e ao desenvolvimento do acervo de Schengen ([274]).

(181) No que diz respeito ao Listenstaine, a presente decisão de execução constitui um desenvolvimento das disposições do acervo de Schengen, na aceção do Protocolo entre a União Europeia, a Comunidade Europeia, a Confederação Suíça e o Principado do Listenstaine relativo à adesão do Principado do Listenstaine ao Acordo entre a União Europeia, a Comunidade Europeia e a Confederação Suíça relativo à associação da Confederação Suíça à execução, à aplicação e ao desenvolvimento do acervo de Schengen ([275]).

([271]) *Opinion 15/2021 regarding the European Commission draft implementing decision pursuant to Directive (EU) 2016/680 on the adequate protection of personal data in the United Kingdom* [Parecer 15/2021 sobre o projeto de decisão de execução da Comissão Europeia nos termos do Regulamento (UE) 2016/680 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-led/opinion-152021-regarding-european--commission-draft_en

([272]) Decisão de Execução (UE) 2020/1745 do Conselho, de 18 de novembro de 2020, relativa à entrada em vigor das disposições do acervo de Schengen em matéria de proteção de dados e à entrada em vigor a título provisório de determinadas disposições do acervo de Schengen na Irlanda (JO L 393 de 23.11.2020, p. 3).

([273]) JO L 176 de 10.7.1999, p. 36.

([274]) JO L 53 de 27.2.2008, p. 52.

([275]) JO L 160 de 18.6.2011, p. 21.

ADOTOU A PRESENTE DECISÃO:

Artigo 1.º

Para efeitos do artigo 36.º da Diretiva (UE) 2016/680, o Reino Unido assegura um nível de proteção adequado dos dados pessoais transferidos da União Europeia para as autoridades públicas do Reino Unido responsáveis pela prevenção, investigação, deteção ou repressão de infrações penais e pela execução de sanções penais.

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 supervisão competentes dos Estados-Membros exerçam as suas competências, nos termos do artigo 47.º da Diretiva (UE) 2016/680, no que respeita às transferências de dados pessoais para autoridades públicas no Reino Unido dentro do 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 e as condições em que os direitos individuais são exercidos, 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 britânica competente, 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 britânicas no direito das pessoas singulares à proteção dos seus 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.

5. The Commission may suspend, repeal or amend this Decision if the lack of cooperation of the government of the United Kingdom prevents the Commission from determining whether the finding in Article 1 is affected.

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 58.º, n.º 2, da Diretiva (UE) 2016/680.

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