Parecer 15/2021 sobre o projeto de decisão de execução da Comissão Europeia nos termos da Diretiva (UE) 2016/680 relativa à adequação do nível de proteção de dados pessoais no Reino Unido

Adotado em 13 de abril de 2021

Translations proofread by EDPB Members.
This language version has not yet been proofread.

Histórico das versões

Versão 1.1	6 de julho de 2021	Alteração da formatação
Versão 1.0	13 de abril de 2021	Adoção do parecer

ÍNDICE

O Comité Europeu para a Proteção de Dados

Tendo em conta o artigo 51.º, n.º 1, alínea g), da 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] (a seguir designada por «Diretiva sobre a Proteção de Dados na Aplicação da Lei»),

Tendo em conta o artigo 12.º e o artigo 22.º do seu regulamento interno,

ADOTOU O SEGUINTE PARECER:

1 RESUMO

1. Em 19 de fevereiro de 2021, a Comissão Europeia aprovou o seu projeto de decisão de execução (a seguir designado por «projeto de decisão») relativo à adequação do nível de proteção de dados pessoais pelo Reino Unido, nos termos da Diretiva sobre a Proteção de Dados na Aplicação da Lei[2]. Posteriormente, a Comissão Europeia iniciou o processo para a sua adoção formal.

2. Na mesma data, a Comissão Europeia solicitou o parecer do Comité Europeu para a Proteção de Dados (a seguir designado por «CEPD»)[3]. A avaliação do CEPD da adequação do nível de proteção oferecido no Reino Unido foi realizada com base no exame do próprio projeto de decisão e com base numa análise da documentação disponibilizada pela Comissão Europeia.

3. O CEPD utilizou como referência principal para este trabalho os seus critérios de referência para a adequação no quadro da Diretiva sobre a Proteção de Dados na Aplicação da Lei[4], adotados em 2 de fevereiro de 2021, bem como a jurisprudência pertinente refletida nas Recomendações 02/2020 sobre as garantias essenciais europeias relativas às medidas de vigilância[5], do CEPD.

4. O objetivo fundamental do CEPD é apresentar um parecer à Comissão Europeia relativo à adequação do nível de proteção oferecido às pessoas singulares no Reino Unido. Convém realçar que o CEPD não espera que o enquadramento jurídico do Reino Unido reproduza a legislação europeia em matéria de proteção de dados.

5. Todavia, o CEPD recorda que o artigo 36.º da Diretiva sobre a Proteção de Dados na Aplicação da Lei e a jurisprudência do Tribunal de Justiça da União Europeia (a seguir designado por «TJUE») exigem que a legislação do país terceiro esteja harmonizada com a essência dos princípios fundamentais consagrados na Diretiva sobre a Proteção de Dados na Aplicação da Lei para se considerar que esta

[1] JO L 119 de 4.5.2016, p. 89.
[2] Ver o comunicado de imprensa da Comissão Europeia, Proteção de dados: Comissão Europeia lança processo sobre a circulação de dados pessoais para o Reino Unido, de 19 de fevereiro de 2021, https://ec.europa.eu/commission/presscorner/detail/pt/ip_21_661.
[3] *Idem*.
[4] Ver Recomendações 01/2021 sobre os critérios de referência para a adequação no quadro da Diretiva sobre a Proteção de Dados na Aplicação da Lei, do CEPD, adotadas em 2 de fevereiro de 2021, https://edpb.europa.eu/system/files/2021-05/recommendations012021onart.36led.pdf_pt.pdf.
[5] Ver Recomendações 02/2020 sobre as garantias essenciais europeias relativas às medidas de vigilância, do CEPD, adotadas em 10 de novembro de 2020, https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-022020-european-essential-guarantees_pt.

oferece um nível adequado de proteção. No domínio da proteção de dados, o CEPD assinala que existe uma harmonização importante entre o quadro da Diretiva sobre a Proteção de Dados na Aplicação da Lei e o quadro jurídico do Reino Unido quanto a determinadas disposições fundamentais, tais como conceitos (por exemplo, «dados pessoais»; «tratamento de dados pessoais». «responsável pelo tratamento»). fundamentos para o tratamento lícito e leal para fins legítimos, limitação das finalidades, qualidade dos dados e proporcionalidade, conservação de dados, segurança e confidencialidade, transparência, categorias especiais de dados, decisões automatizadas e definição de perfis.

6. O CEPD recomenda que a Comissão Europeia complemente a sua análise com informações sobre a existência de um mecanismo que vise informar as autoridades competentes dos Estados-Membros a respeito do tratamento posterior ou da divulgação pelas autoridades do Reino Unido para as quais transferiram os dados pessoais e identificar a sua eficácia nos termos da ordem jurídica do Reino Unido.

7. O CEPD considera que as disposições da parte 3, capítulo 5, do *Data Protection Act 2018* [Lei de 2018 relativa à proteção de dados] (a seguir designada por «DPA 2018»), preveem, em princípio, um nível de proteção essencialmente equivalente ao assegurado pelo direito da UE, no que se refere à transferência de dados pessoais de uma autoridade de aplicação da lei do Reino Unido para um país terceiro.

8. Embora o CEPD assinale a capacidade de o Reino Unido, nos termos do seu quadro jurídico, reconhecer que os territórios oferecem um nível adequado de proteção de dados à luz do quadro de proteção de dados do Reino Unido, o CEPD pretende sublinhar que tal pode resultar em eventuais riscos para a proteção oferecida aos dados pessoais transferidos da UE, especialmente se, no futuro, o quadro de proteção de dados do Reino Unido se desviar do acervo da UE. **No que respeita às situações anteriormente referidas, a Comissão Europeia deve, por conseguinte, cumprir a sua função de controlo e, caso o nível de proteção essencialmente equivalente dos dados pessoais transferidos da UE não seja mantido, a Comissão Europeia deve ponderar a possibilidade de alterar a decisão de adequação, a fim de introduzir garantias específicas para os dados transferidos da UE e/ou suspender a decisão de adequação.**

9. **Por último, relativamente aos acordos internacionais celebrados entre o Reino Unido e países terceiros,** a Comissão Europeia é convidada a examinar a interação entre o quadro de proteção de dados do Reino Unido e os seus compromissos internacionais, em especial, a fim de assegurar a continuidade do nível de proteção quando os dados pessoais são transferidos da UE para o Reino Unido, com base na decisão de adequação do Reino Unido, e são depois transferidos para outros países terceiros, bem como a controlar e a agir de forma contínua, quando necessário, caso a celebração de acordos internacionais entre o Reino Unido e países terceiros possa prejudicar o nível de proteção de dados pessoais oferecido na UE.

10. A este respeito, o CEPD sublinha que a entrada em vigor do acordo entre o Reino Unido e os EUA sobre o acesso a dados eletrónicos para efeitos de combate à criminalidade grave (a seguir designado por «Acordo *CLOUD Act* entre o Reino Unido e os EUA»)[6] pode afetar as transferências ulteriores das

[6] Ver *Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime* [Acordo entre o Governo do Reino Unido da Grã-Bretanha e da Irlanda do Norte e o Governo dos Estados Unidos da América sobre o acesso a dados eletrónicos para efeitos de combate à criminalidade grave], Washington, EUA, 3 de outubro de 2019.

autoridades de aplicação da lei do Reino Unido, em especial, no que se refere à emissão e à transmissão de ordens, nos termos do artigo 5.º do Acordo *CLOUD Act* entre o Reino Unido e os EUA.

11. O CEPD recomenda igualmente que a Comissão Europeia controle de forma contínua se a celebração de futuros acordos com países terceiros para efeitos de cooperação no domínio da aplicação da lei, que prevejam um fundamento jurídico para a transferência de dados pessoais para esses países, poderá afetar as condições para a partilha ulterior das informações recolhidas, em especial, se as disposições desses acordos internacionais forem suscetíveis de afetar a aplicação da legislação do Reino Unido em matéria de proteção de dados e prevejam limitações ou isenções adicionais em relação à utilização posterior e à divulgação no estrangeiro das informações recolhidas para efeitos de aplicação da lei. O CEPD considera que tais informações e avaliações são fundamentais, a fim de permitir uma análise abrangente do nível de proteção oferecido pelo quadro legislativo e pelas práticas do Reino Unido em relação à divulgação no estrangeiro.

2 INTRODUÇÃO

2.1 Quadro do Reino Unido em matéria de proteção de dados

12. O quadro de proteção de dados do Reino Unido baseia-se, em grande medida, no quadro de proteção de dados da UE [em particular na Diretiva sobre a Proteção de Dados na Aplicação da Lei e no 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 (a seguir designado por «RGPD»)], uma vez que o Reino Unido foi Estado-Membro da UE até 31 de janeiro de 2020. Além disso, a DPA 2018, que entrou em vigor em 23 de maio de 2018 e que revogou o *Data Protection Act 1998* [Lei de 1998 relativa à proteção de dados] do Reino Unido, transpõe a Diretiva sobre a Proteção de Dados na Aplicação da Lei através da sua parte 3, especifica a aplicação do RGPD na legislação do Reino Unido, e atribui poderes e impõe deveres à autoridade de controlo da proteção de dados, o gabinete do Comissário para a Informação (a seguir designado por «ICO») do Reino Unido.

13. Tal como mencionado no considerando 12 do projeto de decisão, o Governo do Reino Unido aprovou o *European Union (Withdrawal) Act 2018* [Lei de 2018 relativa à (saída da) União Europeia], que incorpora no direito do Reino Unido o direito da UE diretamente aplicável. Ao abrigo desta lei, os ministros do Reino Unido têm o poder de introduzir atos de direito derivado, por meio de instrumentos estatutários, para proceder às alterações necessárias ao direito da UE mantido na sequência da saída do Reino Unido da União Europeia, a fim de o adaptar ao contexto interno.

14. Consequentemente, o quadro jurídico aplicável no Reino Unido após o fim do período de transição[7] é composto:

- Pelo Regulamento Geral sobre a Proteção de Dados do Reino Unido (a seguir designado por «RGPD do Reino Unido»), conforme incorporado no direito do Reino Unido ao abrigo do *European Union (Withdrawal) Act 2018* e alterado pelos Regulamentos DPPEC [*Data Protection, Privacy and Electronic Communications (Amendment Etc.) (EU Exit)*] [Regulamentos relativos à proteção dos dados, privacidade e comunicações eletrónicas (alterações, etc.) (saída da UE)] de 2019;

[7] O período de transição termina a 31 de dezembro de 2020, data após a qual o direito da UE deixa de ser aplicável no Reino Unido. O «período de ponte» termina, o mais tardar, a 30 de junho de 2021 e refere-se ao período adicional durante o qual a transmissão de dados pessoais da UE para o Reino Unido não é considerada uma transferência.

- Pela DPA 2018, alterada pelos Regulamentos DPPEC de 2019 e de 2020; e ainda
- Pelo *Investigatory Powers Act 2016* [Lei de 2016 relativa aos poderes de investigação] (a seguir designada por «IPA 2016»).

(Em conjunto, designados por «quadro do Reino Unido em matéria de proteção de dados»).

2.2 Âmbito da avaliação do CEPD

15. O projeto de decisão da Comissão Europeia é o resultado de uma avaliação do quadro de proteção de dados do Reino Unido, seguida de conversações com o Governo do Reino Unido. Segundo o artigo 51.º, n.º 1, alínea g), da Diretiva sobre a Proteção de Dados na Aplicação da Lei, prevê-se que o CEPD apresente um parecer independente relativo às conclusões da Comissão Europeia, identifique as insuficiências do quadro de adequação, se as houver, e envide esforços no sentido de elaborar propostas a fim de as resolver.

16. Tal como mencionado nos critérios de referência para a adequação no quadro da Diretiva sobre a Proteção de Dados na Aplicação da Lei, «*as informações da Comissão Europeia devem ser exaustivas e permitir que o CEPD possa proceder à sua própria avaliação do nível de proteção de dados no país terceiro*[8]».

17. A este respeito, importa assinalar que o CEPD não recebeu atempadamente a totalidade dos documentos pertinentes para a análise do quadro jurídico do Reino Unido. O CEPD recebeu a maior parte da legislação do Reino Unido referida no projeto de decisão através de ligações referenciadas neste último. A Comissão Europeia não se encontrava em condições de facultar ao CEPD as explicações e os compromissos escritos, por parte do Reino Unido, pertinentes para este exercício de análise e relativos aos intercâmbios entre as autoridades do Reino Unido e a Comissão Europeia[9].

18. Tendo em conta as considerações anteriores e devido ao prazo limitado (dois meses) concedido ao CEPD para a adoção do presente parecer, o CEPD optou por centrar a sua análise em alguns pontos específicos apresentados no projeto de decisão e pronunciar-se sobre os mesmos. Ao analisar a legislação e as práticas de um país terceiro que foi um Estado-Membro da UE até recentemente, é evidente que o CEPD identificou muitos aspetos como sendo essencialmente equivalentes. Tendo em conta a sua função no processo de adoção de uma decisão de adequação e o volume de legislação e de práticas a analisar, o CEPD decidiu centrar a sua atenção nos aspetos que considerou carecerem de uma análise mais pormenorizada.

19. O CEPD teve em conta o quadro europeu aplicável em matéria de proteção de dados, incluindo os artigos 7.º, 8.º e 47.º da Carta dos Direitos Fundamentais da União Europeia (a seguir designada por

[8] Ver Recomendações 01/2021 sobre os critérios de referência para a adequação no quadro da Diretiva sobre a Proteção de Dados na Aplicação da Lei, n.º 15, p. 5.

[9] Trata-se de elementos em relação aos quais a Comissão Europeia remete, no seu projeto de decisão, para explicações das autoridades do Reino Unido, sem facultar os documentos escritos dessas autoridades que as fundamentam, por exemplo: os efeitos das disposições transitórias e da ausência de uma disposição de caducidade (considerando 87); exemplos de consentimento como um fundamento adequado para o tratamento (nota 68); a definição do termo «inexatos» como dados pessoais «incorretos ou suscetíveis de induzir em erro» (nota 79); o mandato da ISC (nota 245); o baixo limiar para a apresentação de uma reclamação ao IPT e o facto de não ser raro o IPT determinar que o autor da reclamação nunca foi, na verdade, objeto de investigação por uma autoridade pública (nota 263); a combinação de poderes derivada da legislação e do direito comum (nota 52); os poderes de prerrogativa exercidos pelo governo (nota 62); o facto de outras organizações poderem seguir os princípios do Código de Prática MoPI, se o desejarem (nota 86).

«Carta da UE»), que protegem, respetivamente, o direito à vida privada e familiar, o direito à proteção de dados pessoais e o direito à ação e a um tribunal imparcial; e o artigo 8.º da Convenção Europeia dos Direitos Humanos (a seguir designada por «CEDH»), que protege o direito à vida privada e familiar. Para além do anteriormente exposto, o CEPD teve em consideração os requisitos da Diretiva sobre a Proteção de Dados na Aplicação da Lei, bem como a jurisprudência pertinente.

20. O objetivo deste exercício de análise consiste em apresentar à Comissão Europeia um parecer sobre a avaliação da adequação do nível de proteção no Reino Unido. O conceito de «nível de proteção adequado», que já existia na Diretiva 95/46/CE, foi mais desenvolvido pelo TJUE. É importante relembrar a norma definida pelo TJUE no processo «Schrems I», designadamente que, embora o «nível de proteção» num país terceiro deva ser «substancialmente equivalente» ao garantido dentro da UE, «os meios a que esse país recorre para assegurar tal nível de proteção [podem] ser diferentes dos implementados dentro da [UE]»[10]. Por conseguinte, o objetivo não é imitar ponto por ponto a legislação europeia, mas sim estabelecer o essencial e os principais requisitos da legislação em apreciação. A adequação pode ser alcançada através de uma combinação de direitos conferidos aos titulares dos dados e de deveres impostos a quem trata os dados ou quem exerce o controlo sobre esse tratamento e supervisão por organismos independentes. Contudo, as normas relativas à proteção de dados só são eficazes se tiverem caráter executório e forem aplicadas na prática. Por conseguinte, é necessário ter em conta não apenas o conteúdo das normas aplicáveis aos dados pessoais transferidos para um país terceiro ou organização internacional, mas também o sistema existente para assegurar a eficácia dessas normas. A existência de mecanismos executórios eficientes é extremamente importante para a eficácia das normas de proteção de dados[11].

2.3 Preocupações e observações gerais

2.3.1 Compromissos internacionais assumidos pelo Reino Unido

21. Segundo o artigo 36.º, n.º 2, alínea c), da Diretiva sobre a Proteção de Dados na Aplicação da Lei e os critérios de referência para a adequação no quadro da Diretiva sobre a Proteção de Dados na Aplicação da Lei[12], ao avaliar a adequação do nível de proteção de um país terceiro, a Comissão Europeia tem em conta, entre outros, os compromissos internacionais assumidos pelo país terceiro, ou outras obrigações decorrentes da participação do país terceiro em sistemas multilaterais ou regionais, em especial em relação à proteção de dados pessoais, bem como a aplicação de tais obrigações. Além disso, há que ter em conta a adesão do país terceiro em causa à Convenção do Conselho da Europa para a proteção das pessoas relativamente ao tratamento automatizado de dados de caráter pessoal, de 28 de janeiro de 1981 (a seguir designada por «Convenção 108»)[13], e o seu Protocolo Adicional[14].

[10] Ver acórdão do TJUE, de 6 de outubro de 2015, Maximilian Schrems/Data Protection Commissioner (a seguir designado por «Schrems I»), C-362/14, ECLI:EU:C:2015:650, n.os 73 e 74.
[11] Ver Recomendações 01/2021 sobre os critérios de referência para a adequação no quadro da Diretiva sobre a Proteção de Dados na Aplicação da Lei, do CEPD, n.º 14, p. 5.
[12] Ver Recomendações 01/2021 sobre os critérios de referência para a adequação no quadro da Diretiva sobre a Proteção de Dados na Aplicação da Lei, do CEPD, n.º 24, p. 7.
[13] Ver Convenção para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal, Convenção 108, de 28 de janeiro de 1981.
[14] Ver Protocolo Adicional à Convenção para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal, respeitante às Autoridades de Controlo e aos Fluxos Transfronteiriços de Dados, aberto à assinatura em 8 de novembro de 2001.

22. **A este respeito, o CEPD saúda o facto de o Reino Unido ter aderido à CEDH e se encontrar sob a jurisdição do Tribunal Europeu dos Direitos Humanos (TEDH). Além disso, o Reino Unido aderiu igualmente à Convenção 108 e ao seu Protocolo Adicional, assinou a Convenção 108+[15] em 2018 e encontra-se atualmente a trabalhar na sua ratificação.**

2.3.2 Eventual divergência futura do quadro de proteção de dados do Reino Unido

23. Tal como mencionado no considerando 171 do projeto de decisão, a Comissão Europeia deve ter em conta que, com o fim do período de transição previsto no Acordo de Saída[16], o Reino Unido administra, aplica e faz cumprir o seu próprio regime de proteção de dados e, assim que a «disposição de ponte»[17] prevista no artigo FINPROV.10A do Acordo de Comércio e Cooperação UE-Reino Unido[18] deixar de ser aplicável, tal poderá, nomeadamente, envolver alterações ou modificações do quadro de proteção de dados avaliado no projeto de decisão, bem como outros desenvolvimentos pertinentes.

24. Por conseguinte, a Comissão Europeia decidiu incluir uma cláusula de caducidade no seu projeto de decisão[19], que define a data de caducidade para quatro anos após a respetiva entrada em vigor.

25. Importa assinalar que a possibilidade de os ministros do Reino Unido e de o ministro da tutela do Reino Unido introduzirem atos de direito derivado após o fim do «período de ponte» pode futuramente resultar numa divergência significativa do quadro de proteção de dados do Reino Unido em relação ao da UE.

26. Por último, desde o fim do período de transição, o Reino Unido não só deixou de estar vinculado pela jurisprudência do TJUE como também os acórdãos já adotados pelo TJUE, considerados como jurisprudência mantida no quadro jurídico do Reino Unido, podem já não vincular o Reino Unido. Tal deve-se, em especial, ao facto de o Reino Unido ter a possibilidade de, após o final do «período de ponte», modificar o direito da UE mantido e o seu Supremo Tribunal não estar vinculado por qualquer jurisprudência da UE mantida[20].

27. **Tendo em consideração os riscos relacionados com o eventual desvio do quadro de proteção de dados do Reino Unido em relação ao acervo da UE após o fim do «período de ponte», o CEPD saúda a decisão da Comissão Europeia de introduzir uma cláusula de caducidade de quatro anos para o projeto de decisão. Todavia, o CEPD gostaria de sublinhar, no presente documento, a importância da função de controlo da Comissão Europeia[21]. Com efeito, a Comissão Europeia deve controlar todos os desenvolvimentos pertinentes no Reino Unido que possam ter impacto no critério de «equivalência essencial» aplicado ao nível de proteção dos dados pessoais transferidos nos termos da decisão de adequação do Reino Unido, de forma contínua e permanente, a contar da data da sua entrada em vigor. Além disso, a Comissão Europeia deve tomar as medidas adequadas, mediante a**

[15] Ver Protocolo que altera a Convenção para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Caráter Pessoal (a seguir designada por «Convenção 108+»), de 18 de maio de 2018.
[16] Ver 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 (JO L 029 de 31.1.2020, p. 7).
[17] O período de transição termina a 31 de dezembro de 2020, data após a qual o direito da UE deixa de ser aplicável no Reino Unido. O «período de ponte» termina, o mais tardar, a 30 de junho de 2021 e refere-se ao período adicional durante o qual a transmissão de dados pessoais da UE para o Reino Unido não é considerada uma transferência.
[18] Ver 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).
[19] Ver artigo 4.º do projeto de decisão. Ver, igualmente, considerando 172 do projeto de decisão.
[20] Ver secção 6, pontos 3 a 6, do *European Union (Withdrawal) Act 2018*.
[21] Ver artigo 36.º, n.º 4, da Diretiva sobre a Proteção de Dados na Aplicação da Lei.

suspensão, alteração ou revogação da decisão de adequação, com base nas circunstâncias em apreço, se, após a adoção da decisão de adequação, a Comissão Europeia tiver indicações de que deixou de ser assegurado um nível de proteção adequado no Reino Unido.

28. No que lhe diz respeito, o CEPD envidará todos os esforços a fim de informar a Comissão Europeia sobre qualquer medida pertinente tomada pelas autoridades de controlo da proteção de dados dos Estados-Membros (a seguir designadas por «AC») e, em especial, relativamente a reclamações apresentadas na UE por titulares de dados, a respeito da transferência de dados pessoais da UE para o Reino Unido.

3 NORMAS APLICÁVEIS AO TRATAMENTO DE DADOS PESSOAIS PELAS AUTORIDADES COMPETENTES PARA EFEITOS DE APLICAÇÃO DO DIREITO PENAL

3.1 Âmbito material

29. Em relação aos considerandos 24 e seguintes do projeto de decisão, o CEPD assinala que o projeto de decisão de adequação não inclui muitos pormenores relativos às atividades e ao quadro jurídico aplicáveis a outras agências que exercem funções de aplicação da lei que não sejam as autoridades policiais.

30. Por exemplo, o documento *Explanatory Framework for Adequacy Discussions, Section F: Law Enforcement* [Quadro explicativo para as conversações em matéria de adequação, Secção F: Aplicação da Lei][22], do Reino Unido, indica, na página 11, que a ***National Crime Agency*** [agência britânica de combate à criminalidade] (a seguir designada por «NCA») que exerce, nomeadamente, uma função mais ampla em termos de informações criminais, poderia ser uma agência de aplicação da lei de especial interesse. Ao descrever a sua missão, a NCA indica que colige informações a partir de diversas fontes, a fim de maximizar a análise, a avaliação e as oportunidades táticas, nomeadamente, através da interceção técnica de comunicações, de parceiros em matéria de aplicação da lei no Reino Unido e no estrangeiro e de agências de segurança e de informações[23]. A NCA é também um dos principais interlocutores dos parceiros internacionais de aplicação da lei e desempenha um papel fundamental no intercâmbio de informações criminais[24].

[22] Ver *Explanatory Framework for Adequacy Discussions, Section F: Law Enforcement*, do Governo do Reino Unido, 13 de março de 2020, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/872237/F_-_Law_Enforcement_.pdf.

[23] Ver o sítio Web da NCA, «*Intelligence: enhancing the picture of serious organised crime affecting the UK*» [Informações: melhorar o panorama da criminalidade grave organizada que afeta o Reino Unido], https://www.nationalcrimeagency.gov.uk/what-we-do/how-we-work/intelligence-enhancing-the-picture-of-serious-organised-crime-affecting-the-uk.

[24] Embora nem todas as informações tratadas pela NCA sejam dados pessoais, uma parte substancial pode constituir informações pessoais e as atividades aqui descritas diferem das do policiamento clássico, de modo que uma avaliação do acesso a dados pessoais pelas autoridades de aplicação da lei do Reino Unido estaria incompleta sem uma avaliação rigorosa das atividades da NCA. Parece razoável garantir que é atribuído o mesmo significado aos princípios da proteção de dados em todas as agências pertinentes de aplicação da lei, dando assim mais visibilidade a uma agência especializada em análise de dados, como é o caso da NCA. Além disso, na secção «*Looking to the future*» [Perspetivas para o futuro], a NCA continua a explicar que procura continuamente novas oportunidades para recolher, desenvolver e melhorar as capacidades tradicionais, a fim de aumentar a

31. O CEPD refere ainda o facto de o Quartel-General de Comunicações do Governo (a seguir designado por «GCHQ»), cujas atividades se enquadram, em geral, no âmbito da parte 4 da DPA 2018, ou seja, a segurança nacional, assumir igualmente uma função ativa na redução dos danos societais e financeiros causados pela criminalidade grave e organizada ao Reino Unido, trabalhando em estreita colaboração com o Ministério da Administração Interna [«*Home Office*»] do Reino Unido, a NCA, o serviço de fiscalidade e alfândegas do Reino Unido [«*HM Revenue and Customs*» (HMRC)] e outros departamentos governamentais[25]. As atividades do GCHQ estão relacionadas com o combate ao abuso sexual de menores, à fraude, a outros tipos de criminalidade económica, incluindo o branqueamento de capitais, à utilização criminosa da tecnologia, à cibercriminalidade, à imigração ilegal organizada, incluindo o tráfico de seres humanos, e à droga, às armas de fogo e a outras atividades ilícitas de contrabando.

32. **O CEPD apela à Comissão Europeia que complemente a sua análise com uma análise das agências ativas no domínio da aplicação da lei que parecem ter tornado a recolha e a análise de dados, incluindo dados pessoais, um foco das suas operações diárias, em especial a NCA. Além disso, o CEPD convida a Comissão a analisar mais atentamente as agências como o GCHQ, cujas atividades se enquadram tanto no âmbito da aplicação da lei como no da segurança nacional, e o quadro jurídico que lhes é aplicável para o tratamento de dados pessoais.**

3.2 Garantias, direitos e obrigações

3.2.1 Tratamento com base no «consentimento» do titular dos dados

33. O CEPD toma nota de que a Comissão Europeia declara, nos considerandos 37 e 38 do projeto de decisão, que **o recurso ao consentimento** não é considerado pertinente num cenário de adequação, uma vez que, em situações de transferência, os dados não são diretamente recolhidos junto de um titular dos dados com base no consentimento por uma autoridade de aplicação da lei do Reino Unido.

34. A este respeito, o CEPD recorda que o artigo 36.º, n.º 2, alínea a), da Diretiva sobre a Proteção de Dados na Aplicação da Lei exige a avaliação de uma vasta gama de elementos que não se limitam à situação de transferência, incluindo «[o] primado do Estado de direito, o respeito pelos direitos humanos e liberdades fundamentais, a legislação pertinente em vigor, tanto a geral como a setorial, nomeadamente em matéria de [...] direito penal».

35. O consentimento no contexto da aplicação da lei pode ser pertinente como fundamento jurídico para o tratamento de dados, como uma garantia adicional, ou, em termos mais gerais, como base para exercer poderes de investigação que resultem na obtenção de dados pessoais, por exemplo, o consentimento de um terceiro para efetuar buscas nas suas instalações, ou para confiscar o armazenamento de dados.

36. O CEPD assinala, igualmente com base nas informações apresentadas pela Comissão Europeia no considerando 38 do projeto de decisão, que a utilização do consentimento, tal como enquadrado no

quantidade e a qualidade das informações disponíveis para exploração, tanto no Reino Unido como no estrangeiro. No âmbito desta estratégia, a NCA está a desenvolver a nova *National Data Exploitation Capability* [Capacidade nacional de exploração de dados], recorrendo aos poderes conferidos à agência pelo *Crime and Courts Act* [Lei relativa à criminalidade e aos tribunais], a fim de associar, aceder e explorar dados conservados em todos os níveis do governo. [...] Tal aumentará a agilidade e flexibilidade da NCA para dar resposta a novas ameaças e funcionar de uma forma pró-ativa, a fim de recolher e analisar informações relativas a ameaças emergentes, de modo a poder tomar medidas antes de as ameaças se concretizarem.

[25] Ver sítio Web do GCHQ, na página *Mission* [Missão], *Serious and Organised Crime* [Criminalidade grave e organizada], https://www.gchq.gov.uk/section/mission/serious-crime.

regime do Reino Unido, exigiria sempre o recurso a um fundamento jurídico. Tal significa que, mesmo que a polícia possua poderes legais para tratar os dados para efeitos de uma investigação, em determinadas circunstâncias específicas (por exemplo, para recolher uma amostra de ADN), as autoridades policiais podem considerar adequado pedir o consentimento do titular dos dados.

37. **O CEPD convida a Comissão Europeia a analisar, regra geral, a eventual utilização do consentimento num contexto de aplicação da lei, ao avaliar a adequação de um país terceiro nos termos da Diretiva sobre a Proteção de Dados na Aplicação da Lei.**

3.2.2 Direitos individuais

3.2.2.1 Certificados de segurança nacional

38. Segundo a secção 79 da DPA 2018, os responsáveis pelo tratamento podem candidatar-se a certificados de segurança nacional emitidos por um ministro, por um membro do Conselho de Ministros, pelo Procurador-geral [«*Attorney General*»] ou pelo Advogado-geral da Escócia [«*Advocate General for Scotland*»], que certificam que as limitações das obrigações e dos direitos consagrados na parte 3, capítulos 3 e 4, da DPA 2018 são uma medida necessária e proporcionada para a proteção da segurança nacional.

39. Estes certificados visam conferir uma maior segurança jurídica aos responsáveis pelo tratamento e serão provas concludentes de que a segurança nacional é aplicável ao tratamento de dados pessoais. Todavia, há que referir que estes certificados não são obrigatórios a fim de recorrer a limitações de segurança nacional, mas são antes uma medida de transparência[26].

40. O CEPD entende, a partir do anexo 20, secções 17 e 18, da DPA 2018, que um certificado de segurança nacional emitido nos termos do *Data Protection Act 1998* (a seguir designado por «certificado antigo») teve um efeito alargado para o tratamento de dados pessoais até 25 de maio de 2019 nos termos do DPA 2018. Até esta data, salvo se fossem substituídos ou revogados, os certificados antigos eram considerados como se tivessem sido emitidos nos termos da DPA 2018. Todavia, caso não exista uma data de validade expressa num certificado de segurança nacional emitido ao abrigo do *Data Protection Act 1998*, o CEPD entende que esse certificado continuará a ser válido para o tratamento ao abrigo do *Data Protection Act 1998*, salvo se o certificado for revogado ou anulado[27]. Embora a proteção oferecida por estes certificados antigos seja limitada ao tratamento de dados pessoais nos termos do *Data Protection Act 1998*, o CEPD toma nota do facto de que podem ser emitidos novos certificados de segurança nacional nos termos do *Data Protection Act 1998* para dados pessoais tratados nos termos do *Data Protection Act 1998*[28].

41. **Para uma melhor compreensão, o CEPD convida a Comissão Europeia a clarificar, no seu projeto de decisão de adequação, que continua a ser possível emitir certificados de segurança nacional nos termos do *Data Protection Act 1998*. Além disso, o CEPD convida a Comissão Europeia a descrever, no seu projeto de decisão de adequação, os mecanismos de recurso e de supervisão no que diz**

[26] Ver as diretrizes do Ministério da Administração Interna do Reino Unido, *The Data Protection Act 2018, National Security Certificates* [A Lei de 2018 relativa à proteção de dados, Certificados de segurança nacional], p 4, de agosto de 2020, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/910279/Data_Protection_Act_2018_-_National_Security_Certificates_Guidance.pdf.

[27] Ver as diretrizes do Ministério da Administração Interna do Reino Unido, *The Data Protection Act 2018, National Security Certificates*, p. 5, de agosto de 2020.

[28] Ver as diretrizes do Ministério da Administração Interna do Reino Unido, *The Data Protection Act 2018, National Security Certificates*, p. 5, de agosto de 2020.

respeito aos certificados emitidos nos termos do *Data Protection Act 1998*. Por último, o CEPD convida a Comissão Europeia a incluir, no seu projeto de decisão de adequação, o número de certificados existentes emitidos nos termos do *Data Protection Act 1998* e a controlar atentamente este aspeto.

3.2.2.2 Decisões automatizadas nos termos da Diretiva sobre a Proteção de Dados na Aplicação da Lei

42. O CEPD salienta que o artigo 11.º, n.º 3, da Diretiva sobre a Proteção de Dados na Aplicação da Lei proíbe as definições de perfis que conduzam à discriminação de pessoas singulares com base nas categorias especiais de dados pessoais. Todavia, o CEPD assinala que a secção 50 da DPA 2018, que estabelece as regras específicas para as decisões automatizadas, não prevê tal proibição.

43. **Por conseguinte, o CEPD convida a Comissão Europeia a verificar este ponto e a apresentar explicitamente as suas conclusões na sua decisão de adequação. Além disso, o CEPD convida a Comissão Europeia a controlar atentamente os casos relacionados com as decisões automatizadas e a definição de perfis.**

44. Segundo os critérios de referência para a adequação no quadro da Diretiva sobre a Proteção de Dados na Aplicação da Lei, «o direito do país terceiro deve prever as garantias necessárias para os direitos e liberdades do titular dos dados. A este respeito, deve ser igualmente tida em conta a existência de um mecanismo que vise informar as autoridades competentes do Estado-Membro pertinente a respeito de qualquer tratamento posterior, tal como a utilização dos dados transferidos para a definição de perfis em grande escala»[29].

45. **O CEPD convida a Comissão a avaliar este elemento à luz das orientações apresentadas pelo CEPD nos seus critérios de referência.**

3.2.3 Transferências ulteriores

46. Segundo os critérios de referência para a adequação no quadro da Diretiva sobre a Proteção de Dados na Aplicação da Lei, as transferências ulteriores de dados pessoais pelo destinatário inicial para outro país terceiro ou organização internacional não devem prejudicar o nível de proteção, previsto na União, das pessoas singulares cujos dados são transferidos. Por conseguinte, tais transferências ulteriores de dados devem ser permitidas unicamente se for assegurada a continuidade do nível de proteção conferido pelo direito da UE. O CEPD considera que, tal como indicado pela Comissão Europeia na sua avaliação, as disposições da parte 3, capítulo 5, da DPA 2018 e, em especial, a secção 73, preveem, em princípio, um nível de proteção essencialmente equivalente ao assegurado pelo direito da UE, no que se refere à transferência de dados pessoais de uma autoridade de aplicação da lei do Reino Unido para um país terceiro.

47. Em primeiro lugar, a secção 73, n.º 1, alínea b), da DPA 2018 prevê, nomeadamente, que um responsável pelo tratamento não pode transferir dados pessoais para um país terceiro ou para uma organização internacional, *exceto se os dados pessoais tiverem sido inicialmente transmitidos ou disponibilizados de outra forma ao responsável pelo tratamento ou a outra autoridade competente por um Estado-Membro que não seja o Reino Unido, e esse Estado-Membro, ou qualquer pessoa estabelecida nesse Estado-Membro que seja uma autoridade competente para efeitos da Diretiva sobre a Proteção de Dados na Aplicação da Lei, tiver autorizado a transferência segundo a legislação do Estado-Membro.* Tais disposições parecem estar em consonância com os critérios de referência

[29] Ver Recomendações 01/2021 sobre os critérios de referência para a adequação no quadro da Diretiva sobre a Proteção de Dados na Aplicação da Lei, do CEPD, n.os 59, 60 e 61.

para a adequação no quadro da Diretiva sobre a Proteção de Dados na Aplicação da Lei, que preveem que deve ser igualmente tida em conta a existência de um mecanismo que permita às autoridades competentes do Estado-Membro em causa serem informadas e autorizarem essa transferência ulterior de dados. O destinatário inicial dos dados transferidos da UE deve ser responsável e estar em condições de provar que a autoridade competente pertinente do Estado-Membro autorizou a transferência ulterior e que estão previstas garantias adequadas para as transferências ulteriores de dados na ausência de uma decisão de adequação relativa ao país terceiro para o qual os dados seriam ulteriormente transferidos. «Neste contexto, deve ser tida em conta a existência de uma obrigação ou de um compromisso de aplicar os códigos de tratamento pertinentes definidos pelas autoridades dos Estados-Membros que efetuam a transferência»[30].

48. **O CEPD convida a Comissão a avaliar este elemento à luz das orientações apresentadas pelo CEPD nos seus critérios de referência para a adequação no quadro da Diretiva sobre a Proteção de Dados na Aplicação da Lei.**

49. Em segundo lugar, tal como explicado no considerando 81 do projeto de decisão, o ministro da tutela do Reino Unido tem o poder de reconhecer que um país terceiro (ou um território ou um setor de um país terceiro), uma organização internacional, ou uma descrição desse país, território, setor, ou organização assegura um nível adequado de proteção de dados pessoais, após consulta do ICO[31]. Ao avaliar a adequação do nível de proteção, o ministro da tutela do Reino Unido deve ter em consideração os mesmos elementos que a Comissão Europeia é obrigada a avaliar nos termos do artigo 36.º, n.º 2, alíneas a), b) e c), da Diretiva sobre a Proteção de Dados na Aplicação da Lei, interpretados em conjugação com o considerando 67 da mesma diretiva e com a jurisprudência da UE mantida. Tal significa que, ao avaliar a adequação do nível de proteção de um país terceiro, a norma pertinente será se esse país terceiro em questão assegura um nível de proteção «essencialmente equivalente» ao assegurado no Reino Unido. Embora o CEPD assinale a capacidade de o Reino Unido, nos termos da DPA 2018, reconhecer que um território assegura um nível adequado de proteção à luz do quadro de proteção de dados do Reino Unido, o CEPD pretende sublinhar que estes territórios podem não beneficiar, até à data, de uma decisão de adequação emitida pela Comissão Europeia que reconheça um nível de proteção «essencialmente equivalente» ao assegurado na UE. Tal pode resultar em eventuais riscos para a proteção oferecida aos dados pessoais transferidos da UE, especialmente, se o quadro de proteção de dados do Reino Unido se desviar futuramente do acervo da UE. Importa salientar que, em julho de 2020, o processo de referência «Schrems II» do TJUE[32] teve como resultado a invalidação da decisão do Escudo de Proteção da Privacidade dos EUA, uma vez que, segundo o TJUE, não era possível considerar que o quadro jurídico dos EUA oferecesse um nível de proteção essencialmente equivalente em comparação com o da UE. Contudo, os acórdãos já adotados pelo TJUE, considerados como jurisprudência mantida no quadro jurídico do Reino Unido, podem já não vincular o Reino Unido. Tal deve-se, em especial, ao facto de o Reino Unido ter a possibilidade de, após o final do «período de ponte», modificar o direito da UE mantido e o seu Supremo Tribunal não estar vinculado por qualquer jurisprudência da UE mantida[33].

[30] Ver Recomendações 01/2021 sobre os critérios de referência para a adequação no quadro da Diretiva sobre a Proteção de Dados na Aplicação da Lei, do CEPD, n.os 55 e 56.
[31] Ver secção 128, n.º 2, da DPA 2018. Ver, igualmente, *Memorandum of Understanding on the role of the ICO in relation to new UK adequacy assessments* [Memorando de entendimento relativo à função do ICO no que respeita às novas avaliações de adequação do Reino Unido], https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2021/03/secretary-of-state-for-the-department-for-dcms-and-the-information-commissioner-sign-memorandum-of-understanding/.
[32] Ver acórdão do TJUE, de 16 de julho de 2020, Data Protection Commissioner/Facebook Ireland Ltd e Maximillian Schrems (a seguir designado por «Schrems II»), C-311/18, ECLI:EU:C:2020:559.
[33] Ver secção 6, n.os 3, 4, 5 e 6, do *European Union (Withdrawal) Act 2018*.

50. **Por conseguinte, o CEPD convida a Comissão Europeia a controlar atentamente o processo de avaliação da adequação e os critérios das autoridades do Reino Unido em relação a outros países terceiros, em especial, no que diz respeito a países terceiros não reconhecidos como adequados pela UE nos termos da Diretiva sobre a Proteção de Dados na Aplicação da Lei.**

51. Caso a Comissão Europeia considere que o país terceiro considerado adequado pelo Reino Unido não assegura um nível de proteção essencialmente equivalente ao assegurado na UE, em conformidade com o artigo 36.º da Diretiva sobre a Proteção de Dados na Aplicação da Lei, **o CEPD convida a Comissão Europeia a tomar todas e quaisquer medidas necessárias, por exemplo, alterar a decisão de adequação do Reino Unido, a fim de introduzir garantias específicas para os dados pessoais provenientes da UE, e/ou ponderar a suspensão da decisão de adequação do Reino Unido, caso os dados pessoais transferidos da UE para o Reino Unido sejam objeto de transferências ulteriores para o país terceiro em questão com base num regulamento de adequação do Reino Unido**.

52. **Por último, em relação aos acordos internacionais celebrados, ou a celebrar futuramente, pelo Reino Unido e ao eventual acesso a dados pessoais da UE pelas autoridades do(s) país(es) terceiro(s) parte(s) nesses acordos, o CEPD recomenda que a Comissão Europeia examine a interação entre o quadro de proteção de dados do Reino Unido e os seus compromissos internacionais, em especial, a fim de assegurar a continuidade do nível de proteção no caso de transferências ulteriores, para outros países terceiros, de dados pessoais transferidos da UE para o Reino Unido com base numa decisão de adequação do Reino Unido; bem como controlar e agir de forma contínua, quando necessário, no que diz respeito à celebração de acordos internacionais entre o Reino Unido e países terceiros que possam prejudicar o nível de proteção de dados pessoais oferecido na UE.** Por exemplo, embora a Comissão Europeia tenha referido o facto de o Acordo *CLOUD Act* entre o Reino Unido e os EUA[34] poder afetar as transferências ulteriores para os EUA de prestadores de serviços no Reino Unido, **o CEPD sublinha que a entrada em vigor deste acordo pode igualmente afetar as transferências ulteriores de autoridades de aplicação da lei no Reino Unido, em especial, relativamente à emissão e à transmissão de ordens, em conformidade com o artigo 5.º do Acordo *CLOUD Act* entre o Reino Unido e os EUA**.

53. O CEPD considera igualmente que a celebração de futuros acordos com países terceiros para efeitos de cooperação no domínio da aplicação da lei, que prevejam um fundamento jurídico para a transferência de dados pessoais para esses países, pode também afetar significativamente as condições aplicáveis à partilha ulterior das informações recolhidas, uma vez que tais acordos podem afetar o quadro jurídico em matéria de proteção de dados do Reino Unido que foi objeto de avaliação.

54. **Por conseguinte, o CEPD recomenda que a Comissão Europeia controle, de forma contínua, se a celebração de futuros acordos entre o Reino Unido e países terceiros é suscetível de afetar a aplicação da legislação do Reino Unido em matéria de proteção de dados, e preveja limitações ou isenções adicionais em relação à partilha ulterior e à utilização posterior e divulgação no estrangeiro de informações recolhidas para efeitos de aplicação da lei. O CEPD considera que tais informações e avaliações são fundamentais, a fim de permitir uma análise abrangente do nível de proteção oferecido pelo quadro legislativo e pelas práticas do Reino Unido em relação à divulgação no estrangeiro.**

55. Por último, o CEPD toma nota de que, segundo a secção 76, n.º 4, alínea b) [«*Transfers on the basis of special circumstances*» (Transferências com base em circunstâncias especiais)], da DPA 2018, as

[34] Ver *Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime*, Washington, EUA, 3 de outubro de 2019, https://www.gov.uk/government/publications/ukusa-agreement-on-access-to-electronic-data-for-the-purpose-of-countering-serious-crime-cs-usa-no62019.

autoridades de aplicação da lei no Reino Unido podem transferir dados pessoais para um país terceiro ou para uma organização internacional quando a transferência *for necessária para efeitos de obtenção de aconselhamento jurídico em relação a uma das finalidades de aplicação da lei*. **O CEPD salienta que o artigo 38.º da Diretiva sobre a Proteção de Dados na Aplicação da Lei não contém uma disposição correspondente. Por conseguinte, convida a Comissão Europeia a clarificar o que se entende por aconselhamento jurídico e que tipo de dados pessoais são partilhados nesses casos.**

3.2.4 Tratamento posterior, incluindo a partilha ulterior para finalidades de segurança nacional

56. Nos seus critérios de referência para a adequação no quadro da Diretiva sobre a Proteção de Dados na Aplicação da Lei, o CEPD assinalou que, no que respeita ao tratamento posterior, ou à divulgação de dados transferidos da UE para outras finalidades que não as de aplicação da lei, tais como finalidades de segurança nacional, este deve ser igualmente previsto por lei, necessário e proporcionado. Tal como avaliado pela Comissão Europeia no seu projeto de decisão, a secção 36, n.º 3, da DPA 2018, o *Digital Economy Act 2017* [Lei de 2017 relativa à economia digital], o *Crime and Courts Act 2013* [Lei de 2013 relativa à criminalidade e aos tribunais] e o *Serious Crime Act 2017* [Lei de 2017 relativa à criminalidade grave] preveem um quadro jurídico claro que permite a partilha ulterior, desde que tal partilha ulterior esteja em conformidade com as regras estabelecidas na DPA 2018.

57. O CEPD assinala que, no contexto do tratamento posterior para outras finalidades de dados pessoais transferidos da UE, a Comissão Europeia não avaliou se existem mecanismos que permitam às autoridades de aplicação da lei do Reino Unido informar as autoridades competentes dos Estados-Membros pertinentes quanto a um eventual tratamento posterior de dados. Contudo, os critérios de referência para a adequação no quadro da Diretiva sobre a Proteção de Dados na Aplicação da Lei consideram estes mecanismos como um elemento que deve ser tido em conta[35]. Além disso, a existência de tal mecanismo que vise informar as autoridades competentes dos Estados-Membros a respeito do tratamento posterior de dados para efeitos de aplicação da lei é igualmente considerada como um elemento a ter em conta nos termos dos critérios de referência para a adequação no quadro da Diretiva sobre a Proteção de Dados na Aplicação da Lei[36].

58. **Assim, o CEPD convida a Comissão Europeia a complementar a sua análise com informações relativas à existência de mecanismos que permitam às autoridades de aplicação da lei do Reino Unido notificar as autoridades competentes dos Estados-Membros pertinentes quanto a um eventual tratamento posterior de dados transferidos da UE.**

59. Além disso, 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, o fundamento jurídico que autoriza essa partilha é o *Counter-Terrorism Act 2008* [Lei de 2008 relativa ao combate ao terrorismo]. A este respeito, o CEPD assinala que o âmbito e as disposições da secção 19 do *Counter-Terrorism Act 2008* não são totalmente abordados na avaliação da Comissão Europeia e podem implicar uma utilização posterior de natureza mais ampla, em especial, no que diz respeito à secção 19, n.º 2, da *Counter-Terrorism Act 2008*, que prevê que as informações obtidas por um dos serviços de informações em relação ao exercício de uma das suas funções podem ser utilizadas por esse serviço em relação ao exercício de qualquer uma das suas outras funções. A este respeito, o CEPD sublinha que, quando são objeto de tratamento posterior ou de divulgação, os dados devem beneficiar do

[35] Ver Recomendações 01/2021 sobre os critérios de referência para a adequação no quadro da Diretiva sobre a Proteção de Dados na Aplicação da Lei, do CEPD, n.º 41 e nota 39.
[36] Ver Recomendações 01/2021 sobre os critérios de referência para a adequação no quadro da Diretiva sobre a Proteção de Dados na Aplicação da Lei, do CEPD, n.º 40.

mesmo nível de proteção que quando foram inicialmente tratados pela autoridade competente que os recebeu.

3.3 Supervisão e execução coerciva

60. O CEPD assinala que a supervisão das agências de aplicação do direito penal é assegurada por uma combinação de diferentes comissários, para além do ICO. O projeto de decisão de adequação refere o comissário para os poderes de investigação (a seguir designado por «IPC»), o comissário para a conservação e utilização de materiais biométricos, bem como o comissário para as câmaras de videovigilância. Neste contexto, imposta assinalar que o TJUE sublinhou reiteradamente a necessidade de uma supervisão independente. O IPC reveste-se de especial importância em matéria de acesso a dados pessoais transferidos para o Reino Unido. No entendimento do CEPD, o IPC é um «comissário judicial», tal como outros comissários judiciais, a referir no contexto do capítulo sobre segurança nacional, e esses comissários judiciais gozam da independência dos juízes quando exercem também o cargo de comissários. Quanto ao gabinete do IPC, a Comissão Europeia explica, no considerando 245 do projeto de decisão, que funciona como um organismo público independente, embora seja simultaneamente financiado pelo Ministério da Administração Interna do Reino Unido.

61. Além disso, o IPC é igualmente competente para efeitos de supervisão *ex post* das medidas de vigilância. Parece que nesta função, contudo, o papel do IPC é apresentar recomendações em casos de incumprimento e notificar o titular dos dados se o erro for grave e se for do interesse público que a pessoa seja informada.

62. O CEPD não encontrou indicações adicionais no projeto de decisão para avaliar a independência do comissário para a conservação e utilização de materiais biométricos, bem como do comissário para as câmaras de videovigilância.

63. **A Comissão Europeia é convidada a avaliar mais aprofundadamente a independência dos comissários judiciais, igualmente nos casos em que o comissário (já) não exerça funções de juiz, bem como a avaliar a independência do comissário para a conservação e utilização de materiais biométricos e do comissário para as câmaras de videovigilância.**