Parecer 28/2025 relativo ao projeto de decisão de execução da Comissão Europeia nos termos do Regulamento (UE) 2016/679 sobre a adequação do nível de proteção de dados pessoais pelo Brasil

Versão 1.0

Adotado em 04 novembro 2025

Translations proofread by EDPB Members.

This language version has not yet been proofread.

ADOTADO

Resumo

Em 5 de setembro de 2025, a Comissão Europeia deu início ao processo de adoção do seu projeto de decisão de execução («projeto de decisão») sobre a adequação do nível de proteção de dados pessoais pela República Federativa do Brasil («Brasil»).

Em 5 de setembro de 2025, a Comissão Europeia solicitou o parecer do Comité Europeu para a Proteção de Dados (CEPD). A avaliação do CEPD sobre a adequação do nível de proteção conferido pelo Brasil foi efetuada com base na análise do próprio projeto de decisão, bem como numa análise da documentação disponível ao público nos sítios Web oficiais das autoridades brasileiras.

O CEPD centrou-se na avaliação dos aspetos gerais do RGPD constantes do projeto de decisão e no acesso de autoridades públicas a dados pessoais transferidos do EEE para efeitos de aplicação da lei e de segurança nacional, incluindo as vias de recurso disponíveis para as pessoas singulares no EEE. O CEPD avaliou igualmente se as garantias previstas no quadro jurídico do Brasil estão em vigor e são eficazes.

O CEPD utilizou como referência principal para este trabalho o Documento de referência relativo à adequação adotado em 28 de novembro de 2017 pelo Grupo de Trabalho do Artigo 29.º[2], com a última redação que lhe foi dada e adotado em 6 de fevereiro de 2018 pelo CEPD («Documento de referência relativo à adequação»), e as Recomendações 02/2020 do CEPD sobre as garantias essenciais europeias relativas às medidas de vigilância.

O CEPD assinala com agrado que o quadro de proteção de dados, em especial a Lei Geral de Proteção de Dados Pessoais («LGPD») no Brasil, juntamente com decretos presidenciais e regulamentos vinculativos emitidos pela autoridade de proteção de dados do Brasil (Agência Nacional de Proteção de Dados, «ANPD»), estabelecem requisitos (nomeadamente em relação aos princípios, aos direitos dos titulares dos dados, às transferências, à supervisão e ao recurso) que estão estreitamente alinhados com o RGPD e a jurisprudência do Tribunal de Justiça da União Europeia («TJUE»).

O CEPD concluiu igualmente que, no projeto de decisão, a Comissão Europeia deve clarificar determinados aspetos do quadro jurídico do Brasil e acompanhar de perto a sua evolução.

Em relação ao princípio da responsabilização e aos requisitos para a avaliação de impacto sobre a proteção de dados («AIPD»), o CEPD considera importante a obrigação de a realizar nos casos em que o tratamento possa resultar num elevado risco para os direitos e liberdades das pessoas singulares e que a AIPD abranja a avaliação da necessidade e da proporcionalidade do tratamento. Por conseguinte, o CEPD convida a Comissão Europeia a acompanhar a aplicação prática destes requisitos.

[1] 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.

[2] Grupo de Trabalho do Artigo 29.º, WP 254 rev.01, adotado em 28 de novembro de 2017, última redação revista e adotada em 6 de fevereiro de 2018, aprovado pelo CEPD.

A LGPD prevê uma limitação à prestação de informações aos titulares dos dados ou à autoridade de controlo com base nos «segredos comercial e industrial» em determinados casos. Tendo em conta a importância dos requisitos de transparência para a possibilidade de os titulares dos dados controlarem a forma como os seus dados são tratados, bem como a importância das obrigações de cooperação com a autoridade de controlo, em especial de facultar as informações necessárias para as suas funções de supervisão, o CEPD convida a Comissão Europeia a acompanhar a aplicação destas limitações na prática, a fim de compreender melhor o seu impacto nos direitos de informação e de acesso, bem como nos poderes da ANPD, se for caso disso.

Em relação às regras relativas às transferências ulteriores, o CEPD convida a Comissão Europeia a clarificar, no projeto de decisão, se as transferências só podem ser efetuadas em conformidade com condições equivalentes às previstas no artigo 49.º do RGPD, em circunstâncias excecionais nas quais não seja possível utilizar outros instrumentos de transferência. A Comissão é igualmente convidada a esclarecer se os titulares dos dados são informados sobre: eventuais riscos da transferência quando esta se baseia no seu consentimento e nas circunstâncias da transferência (duração e finalidade da transferência, países de destino, responsabilidades das partes envolvidas, direitos dos titulares dos dados e meios para os exercer), independentemente do instrumento de transferência utilizado.

Além disso, o CEPD convida a Comissão Europeia a pormenorizar as funções do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade e a sua interação com a ANPD.

No que diz respeito ao acesso e à utilização, por autoridades públicas brasileiras, de dados pessoais transferidos para responsáveis pelo tratamento e subcontratantes no Brasil para efeitos de aplicação do direito penal e de segurança nacional («acesso governamental»), o CEPD observa que a LGPD não se aplica ao tratamento de dados efetuado para fins *exclusivos* de segurança pública, defesa nacional, segurança do Estado ou investigação e repressão de infrações penais. Ao mesmo tempo, o CEPD assinala com agrado que, na sua jurisprudência, o Supremo Tribunal Federal do Brasil interpretou a LGPD de uma forma que alargou a sua aplicabilidade parcial ao tratamento de dados pessoais para efeitos de investigações criminais e manutenção da ordem pública.

À luz do que precede, o CEPD convida a Comissão a avaliar e clarificar mais aprofundadamente, no projeto de decisão, a aplicabilidade da LGPD em caso de tratamento de dados pessoais para efeitos de aplicação do direito penal, incluindo os poderes de investigação e de correção da ANPD perante as autoridades responsáveis pela aplicação da lei, bem como a ter cuidadosamente em conta qualquer evolução pertinente a este respeito no âmbito da sua obrigação de acompanhamento.

Tendo em conta o facto de ser concedida aos Estados uma ampla margem de apreciação na definição das questões de segurança nacional, o que permite, subsequentemente, isenções no domínio da segurança nacional aquando do tratamento de dados pessoais, o CEPD convida a Comissão a descrever e explicar de forma mais pormenorizada, no projeto de decisão, as linhas gerais do conceito de segurança nacional ao abrigo da legislação brasileira. Neste contexto, o CEPD convida a Comissão a clarificar melhor a forma como as isenções constantes da LGPD para efeitos de segurança nacional se relacionam com a

Índice

O Comité Europeu para a Proteção de Dados,

Tendo em conta o artigo 70.º, n.º 1, alínea s), do 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 (a seguir designado por «RGPD»),

Tendo em conta o Acordo sobre o Espaço Económico Europeu (a seguir designado por «EEE»), nomeadamente o anexo XI e o Protocolo n.º 37, com a redação que lhe foi dada pela Decisão do Comité Misto do EEE n.º 154/2018, de 6 de julho de 2018[3],

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

ADOTOU O SEGUINTE PARECER:

[3] As referências a «Estados-Membros» no presente parecer devem ser entendidas como referências a «Estados do EEE».

1. INTRODUÇÃO

(1) O capítulo V do RGPD estabelece as condições aplicáveis às transferências de dados pessoais para um país terceiro ou para uma organização internacional. As transferências de dados pessoais podem ter lugar com base numa decisão de adequação da Comissão Europeia (artigo 45.º do RGPD) ou, na ausência dessa decisão de adequação, se o responsável pelo tratamento ou o subcontratante proporcionar garantias adequadas, incluindo direitos oponíveis e vias de recurso para o titular dos dados (artigo 46.º do RGPD). Na ausência de uma decisão de adequação ou de garantias adequadas, uma transferência ou um conjunto de transferências para um país terceiro ou uma organização internacional só pode ter lugar em determinadas condições (artigo 49.º do RGPD).

(2) O CEPD recorda que as decisões de adequação reconhecem a proteção contínua dos dados pessoais transferidos do EEE para países terceiros ou organizações internacionais e constituem um instrumento de transferência sólido para assegurar a salvaguarda dos direitos do titular dos dados quando estes são transferidos para fora do EEE. De acordo com o Documento de referência relativo à adequação[4] e com a jurisprudência pertinente do TJUE[5], embora o país terceiro não tenha de proporcionar um nível de proteção idêntico ao garantido na ordem jurídica da União, a expressão «nível de proteção adequado» constante do artigo 45.º, n.º 1, do RGPD deve ser entendida no sentido de que exige que esse país terceiro assegure efetivamente, por força da sua legislação interna ou dos seus compromissos internacionais, um nível de proteção dos direitos e liberdades fundamentais essencialmente equivalente ao garantido na União Europeia, lido à luz da Carta dos Direitos Fundamentais.

(3) O Brasil é uma República Federativa composta pela união dos seus 26 estados e do Distrito Federal, conforme estabelecido na sua Constituição Federal («Constituição»)[6]. Os estados brasileiros possuem também as suas próprias constituições, que não devem contradizer a Constituição Federal. A privacidade e a proteção de dados são protegidas na Constituição enquanto direitos fundamentais (artigo 5.º, ponto X, artigo 5.º, ponto XII, e artigo 5.º, ponto LXXIX da Constituição)[7] e reconhecidas pelo Tribunal Constitucional para qualquer pessoa, incluindo um estrangeiro, independentemente de essa pessoa ser ou não residente no Brasil[8].

(4) O principal ato legislativo que rege a proteção de dados é a Lei Geral de Proteção de Dados Pessoais (LGPD) (Lei n.º 13.709, de 14 de agosto de 2018, com a última redação que lhe foi dada pela Lei n.º 14.460, de 25 de outubro de 2022). A LGPD é completada por decretos vinculativos (Decreto Presidencial n.º 10.474, de 26 de agosto de 2020, e Decreto Presidencial n.º 11.758, de 30 de outubro de 2023), que são juridicamente vinculativos e possuem caráter executório[9].

(5) Para além da LGPD, o quadro de proteção de dados brasileiro inclui regulamentos vinculativos emitidos pela autoridade de proteção de dados do Brasil (Agência Nacional de

[4] Grupo de Trabalho do Artigo 29.º, WP 254 rev.01, adotado em 28 de novembro de 2017, última redação revista e adotada em 6 de fevereiro de 2018, aprovado pelo CEPD, capítulo 3, secção C.
[5] Acórdão do Tribunal de Justiça de 6 de outubro de 2015, Maximillian Schrems/Data Protection Commissioner, processo C-362/14, ECLI:EU:C:2015:650 («acórdão Schrems»); e acórdão do Tribunal Geral de 3 de setembro de 2025, Philippe Latombe/Comissão Europeia, processo T-553/23, ECLI:EU:T:2025:831 («acórdão Latombe»).
[6] Ver considerando 7 do projeto de decisão.
[7] Ver considerando 8 do projeto de decisão.
[8] Ver considerando 9 do projeto de decisão.
[9] Ver considerandos 11 e 12 do projeto de decisão.

Proteção de Dados, «ANPD»)[10]. Estes regulamentos preveem regras adicionais sobre a interpretação e a aplicação da LGPD[11]. Por exemplo, o Regulamento n.º 4, de 24 de fevereiro de 2024, relativo à aplicação de sanções administrativas, o Regulamento n.º 15, de 24 de abril de 2024, relativo à comunicação de incidentes de segurança («Regulamento de Comunicação de Incidente de Segurança»), o Regulamento n.º 19, de 23 de agosto de 2024, relativo à transferência internacional de dados pessoais («Regulamento Transferência de Dados»), o Regulamento n.º 2, de 27 de janeiro de 2022, relativo à aplicação da LGPD às pequenas e médias empresas, o Regulamento n.º 18, de 15 de julho de 2024, relativo ao papel do encarregado da proteção de dados («Regulamento Encarregado da Proteção de Dados»).

(6) O CEPD congratula-se com o reconhecimento constitucional dos direitos à privacidade e à proteção de dados como direitos fundamentais, aplicados através do direito nacional. Além disso, o CEPD regista com agrado os compromissos internacionais assumidos pelo Brasil[12].

(7) O CEPD assinala que, nos termos dos artigos 47.º e 94.º do Regulamento (UE) 2018/1725[13], as instituições, órgãos e organismos da União Europeia podem transferir dados pessoais para um país terceiro, território, setor ou organização internacional reconhecidos pela Comissão Europeia nos termos do artigo 45.º, n.º 3, do Regulamento (UE) 2016/679 como assegurando um nível de proteção adequado, desde que a transferência sirva exclusivamente funções da competência do responsável pelo tratamento, sem necessidade de autorização adicional. O CEPD convida a Comissão Europeia a recordar, nos considerandos do projeto de decisão, esta possibilidade jurídica.

2. ASPETOS GERAIS DA PROTEÇÃO DE DADOS

2.1 Responsabilização e governação dos dados

(8) A LGPD prevê o princípio da responsabilização como um dos princípios gerais aplicáveis ao tratamento de dados pessoais. Segundo a LGPD, os responsáveis pelo tratamento e os subcontratantes[14] devem adotar medidas técnicas e organizativas adequadas para cumprir eficazmente as suas obrigações em matéria de proteção de dados e devem poder demonstrar esse cumprimento, entre outros, à autoridade de controlo competente (artigo 46.º da LGPD). O CEPD observa que essas medidas incluem a designação de um encarregado da proteção de dados (artigo 41.º da LGPD), conforme especificado mais pormenorizadamente no Regulamento Encarregado da Proteção de Dados da ANPD; a avaliação de impacto sobre a proteção de dados (artigo 38.º da LGPD), bem como a manutenção de registos das atividades de tratamento de dados (artigo 37.º da LGPD). Além disso, a LGPD estabelece que os responsáveis pelo tratamento e os subcontratantes podem formular regras internas em

[10] Todos os regulamentos vinculativos emitidos pela ANPD podem ser consultados em: https://www.gov.br/anpd/pt-br/acesso-a-informacao/institucional/atos-normativos/regulamentacoes_anpd.
[11] Ver considerando 13 do projeto de decisão.
[12] Ver considerandos 8 a 10 do projeto de decisão.
[13] Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho, de 23 de outubro de 2018, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos e organismos da União e à livre circulação desses dados, e que revoga o Regulamento (CE) n.º 45/2001 e a Decisão n.º 1247/2002/CE (JO L 295 de 21.11.2018, p. 39).
[14] Agentes de tratamento, nos termos do artigo 5.º, ponto IX, da LGPD.

matéria de boas práticas e modelos de governação, incluindo planos para atividades educativas, mecanismo de supervisão interna e atenuação dos riscos (artigo 50.º da LGPD). O CEPD assinala com agrado que esses instrumentos são semelhantes aos previstos no RGPD para aplicar o princípio da responsabilização e congratula-se com esse estreito alinhamento.

(9) O CEPD observa que, no que diz respeito à AIPD, a LGPD não inclui uma obrigação clara de a realizar nos casos em que o tratamento possa resultar num elevado risco para os direitos e liberdades das pessoas singulares, em que apenas se refere ao eventual pedido da ANPD. A este respeito, o CEPD observa que a ANPD recomenda, nas «perguntas frequentes»[15] relacionadas com a AIPD («perguntas frequentes relativas à AIPD»), a realização de AIPD quando a atividade de tratamento possa resultar num risco elevado. Além disso, a LGPD não inclui explicitamente a avaliação da necessidade e da proporcionalidade no âmbito da AIPD. Todavia, as perguntas frequentes relativas à AIPD recomendam que os responsáveis pelo tratamento e os subcontratantes avaliem, nas suas AIPD, a necessidade e a proporcionalidade do tratamento.

(10) Neste contexto, o CEPD convida a Comissão Europeia a acompanhar a aplicação prática destes requisitos, a fim de verificar se a AIPD é realizada quando a atividade de tratamento pode resultar num elevado risco para os direitos e liberdades das pessoas singulares e se a avaliação da necessidade e da proporcionalidade das atividades de tratamento em relação às finalidades também está incluída nas AIPD.

2.2 Âmbito de aplicação e definições

(11) O capítulo 3 do Documento de referência relativo à adequação é dedicado aos «princípios fundamentais» e refere-se aos conceitos e princípios básicos em matéria de proteção de dados. Um sistema de um país terceiro ou de uma organização internacional deve conter esses conceitos e princípios básicos, a fim de assegurar um nível de proteção dos dados pessoais essencialmente equivalente ao garantido pelo direito da UE. Não têm de imitar a terminologia do RGPD, mas devem refletir e ser coerentes com os conceitos consagrados na legislação da UE em matéria de proteção de dados. O Documento de referência relativo à adequação refere-se aos seguintes conceitos importantes: «dados pessoais», «tratamento», «responsáveis pelo tratamento», «subcontratante», «destinatário» e «dados sensíveis». Este aspeto da lei brasileira será comentado nos parágrafos seguintes.

2.2.1 Âmbito de aplicação material e territorial da LGPD

(12) O CEPD congratula-se com o facto de o âmbito de aplicação da LGPD, tanto material como territorial, ser muito semelhante ao previsto no quadro de proteção de dados da UE.

(13) O artigo 4.º da LGPD exclui do seu âmbito de aplicação o tratamento para fins exclusivamente particulares e não económicos e essas exceções também estão previstas no RGPD [artigo 2.º, n.º 2, alínea c), do RGPD]. Além disso, algumas outras atividades de tratamento não são parcialmente abrangidas pelo âmbito de aplicação da LGPD, nomeadamente o tratamento realizado para: segurança pública, defesa nacional, segurança do Estado ou investigação e repressão de infrações penais; fins jornalísticos e artísticos; investigação

[15] https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/relatorio-de-impacto-a-protecao-de-dados-pessoais-ripd.

académica; investigação no domínio da saúde (artigo 3.º, ponto III, da LGPD). Este aspeto é descrito de forma mais pormenorizada na secção 3.1 do presente parecer.

(14) No que diz especificamente respeito à aplicação parcial da LGPD ao tratamento de dados pessoais efetuado para fins jornalísticos e artísticos, o CEPD observa que o âmbito de aplicação da exceção é equivalente ao estabelecido no artigo 85.º, n.º 2, do RGPD[16], ou seja, essa exceção só se aplica quando os dados pessoais são tratados exclusivamente para esse fim e todas as restantes atividades de tratamento realizadas pela imprensa, por meios de comunicação social e por organismos artísticos são abrangidas pelo âmbito de aplicação da LGPD. Além disso, continuam a ser aplicáveis algumas exceções previstas para o tratamento de dados pessoais exclusivamente para fins académicos, ou seja, os artigos 7.º (requisitos em termos de fundamentos jurídicos) e 11.º (regras relativas ao tratamento de dados sensíveis) da LGPD[17]. O âmbito destas exceções está também em consonância com o estabelecido no artigo 85.º, n.º 2, do RGPD.

2.2.2 Definições

(15) O CEPD assinala com agrado o alinhamento com o quadro da UE em matéria de proteção de dados, no que se refere às definições utilizadas na LGPD, que são coerentes com as previstas no RGPD. Em especial, a LGPD define «dado pessoal», «pseudonimização», «dado anonimizado» [18], «tratamento de dados», «responsável pelo tratamento», «subcontratante» e «dados sensíveis» (artigo 5.º da LGPD) de forma semelhante àquela através da qual são definidos no RGPD, a saber, o considerando 26, o artigo 4.º e o artigo 9.º, n.º 1. Outras definições, por exemplo, «titular dos dados», «encarregado da proteção de dados», «consentimento», «avaliação de impacto sobre a proteção de dados» [19] e um conceito de «responsabilidade conjunta pelo tratamento», são também essencialmente equivalentes aos conceitos previstos no RGPD.

2.3 Princípios e bases jurídicas em matéria de proteção de dados

2.3.1 Princípios do tratamento

(16) O Documento de referência relativo à adequação, em conformidade com o RGPD, estabelece que os dados devem ser tratados de forma lícita, leal e legítima. Nos termos do artigo 6.º da LGPD, as atividades de tratamento de dados pessoais devem ser realizadas de boa-fé e estar sujeitas aos seguintes princípios: finalidade, adequação, necessidade, livre acesso [20], qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas.

[16] Ver também o considerando 35 do projeto de decisão.
[17] Ver também os considerandos 32 e 33 do projeto de decisão.
[18] O artigo 12.º da LGPD especifica ainda que os dados anonimizados não são considerados dados pessoais, salvo quando o processo de anonimização ao qual foram submetidos for revertido ou quando, com esforços razoáveis, puder ser revertido. Este artigo explica que o termo «razoável» deve ser considerado tendo em conta fatores objetivos, tais como: 1) custo e tempo necessários para reverter o processo; 2) as tecnologias disponíveis; e 3) a utilização exclusiva de meios próprios de um responsável pelo tratamento.
[19] Ver o artigo 42.º, n.º 1, ponto I, da LGPD.
[20] «[L]ivre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais» (artigo 6.º, ponto IV, da LGPD).

(17) Tendo em conta os conceitos destes princípios, o sistema jurídico brasileiro consagra os mesmos princípios de tratamento de dados que os estabelecidos no artigo 5.º do RGPD. Por exemplo, no que respeita à limitação da finalidade, a LGPD prevê, no artigo 7.º, n.º 7, que «[o] tratamento posterior dos dados pessoais a que se referem os §§ 3º [tratamento de dados pessoais cujo acesso é público] e 4º [dados tornados manifestamente públicos pelo titular] deste artigo poderá ser realizado para novas finalidades, desde que observados os propósitos legítimos e específicos para o novo tratamento e a preservação dos direitos do titular, assim como os fundamentos e os princípios previstos nesta Lei».

(18) O RGPD exige claramente que esse tratamento posterior só tenha lugar se essa nova finalidade for compatível com a finalidade inicial. O requisito de assegurar a compatibilidade das finalidades (bem como o cumprimento dos padrões éticos aplicáveis e das garantias técnicas e jurídicas) é salientado no documento *Guia orientativo — Tratamento de dados pessoais para fins acadêmicos e para a realização de estudos e pesquisas*, emitido pela ANPD, bem como nas orientações sobre o interesse legítimo. A ANPD, nas orientações sobre o interesse legítimo, explica de que forma o responsável pelo tratamento deve demonstrar uma ligação efetiva entre as duas finalidades do tratamento e ter em conta as «expectativas legítimas» do titular dos dados. Estas orientações esclarecem ainda que «[a] análise da legítima expectativa pode se basear em diversos fatores, entre os quais podem ser destacados: […] d) a finalidade pretendida da [recolha] dos dados e a sua compatibilidade com o tratamento baseado no legítimo interesse». O CEPD congratula-se com essa clarificação pela ANPD, que ajuda a alinhar melhor os requisitos da limitação das finalidades.

(19) O princípio da limitação da conservação previsto no RGPD estipula que os dados só devem ser conservados durante o período necessário para assegurar as finalidades para as quais são tratados [artigo 5.º, n.º 1, alínea e), do RGPD]. Embora o artigo 6.º da LGPD não inclua explicitamente o princípio da limitação da conservação, este artigo deve ser lido em conjugação com o artigo 15.º da LGPD, que especifica o requisito em caso de término do tratamento de dados. Neste artigo, o princípio da limitação da conservação está claramente ligado aos princípios da «adequação» e da «necessidade» que se enquadram nos princípios gerais enumerados no artigo 6.º da LGPD. Para maior clareza, o CEPD incentiva a Comissão Europeia a clarificar, no projeto de decisão, a interação dos artigos 6.º e 15.º da LGPD em relação ao princípio da limitação da conservação.

(20) Além disso, no que diz respeito aos requisitos de limitação da conservação, o artigo 16.º da LGPD estabelece as condições para a conservação e o apagamento de dados pessoais após o término do tratamento. Este artigo prevê igualmente quatro finalidades pelas quais os dados podem ser conservados após o término do seu tratamento: 1) para o cumprimento de obrigações legais ou regulamentares; 2) para fins de investigação, garantindo, sempre que possível, a anonimização dos dados; 3) quando transferidos para terceiros em conformidade com os requisitos da LGPD; ou 4) quando utilizados exclusivamente pelo responsável pelo tratamento, desde que os dados sejam anonimizados e o acesso a esses dados por terceiros seja proibido. O CEPD observa que estas situações de tratamento estão em consonância com o princípio da limitação da conservação consagrado no RGPD.

(21) O princípio da transparência e da lealdade procura assegurar que os titulares dos dados têm controlo sobre os seus dados pessoais e, para o efeito, as informações devem ser facultadas ao titular dos dados de forma proativa[21]. Por seu lado, a LGPD estabelece uma limitação a este princípio no que diz respeito aos «segredos comercial e industrial» que pode ter um

[21] Este aspeto é igualmente salientado pelo Documento de referência relativo à adequação; ver capítulo 3, secção A, ponto 7.

impacto para os titulares dos dados receberem informações sobre o tratamento dos seus dados, a fim de poderem exercer o seu controlo sobre o mesmo (por exemplo, através da apresentação da reclamação à ANPD). Todavia, a Comissão Europeia, no projeto de decisão, explica que esta limitação deve ser interpretada à luz da Lei relativa ao acesso a informações e do Decreto Presidencial n.º 7.721, de 16 de maio de 2012, e por conseguinte, deve ser interpretada «de forma que o tratamento e a divulgação de informações não revelem o segredo comercial nem criem vantagens competitivas para outros intervenientes, cumprindo simultaneamente os objetivos de proteção dos dados pessoais. Tal significa que, no que diz respeito ao princípio da transparência, e em todo o texto da LGPD, a limitação dos "segredos comercial e industrial" não deve ser entendida como um motivo genérico de recusa do cumprimento da lei, mas sim que devem ser estabelecidas garantias específicas para assegurar a divulgação de informações de uma forma que proteja esses interesses»[22].

(22) Tendo em conta a importância do princípio da transparência, o CEPD convida a Comissão Europeia a acompanhar a aplicação desta disposição na prática, a fim de compreender melhor o seu impacto no direito de informação e de acesso.

2.3.2 Medidas de segurança e violações

(23) A LGPD inclui os princípios da segurança e da prevenção, que exigem a aplicação de medidas de proteção dos dados pessoais e de prevenção de danos relacionados com esse tratamento (artigo 6.º, pontos VII e VII, da LGPD). Além disso, a LGPD afirma explicitamente que, quando as medidas de segurança não são adequadamente aplicadas, o tratamento de dados é considerado ilícito. A lei exige que sejam aplicadas as medidas necessárias para demonstrar a conformidade com este princípio através da abordagem baseada no risco (artigos 44.º, 46.º e 47.º da LGPD) e cumprir os requisitos para a avaliação e notificação de violações (artigos 48.º e 49.º da LGPD). O CEPD assinala com agrado que esses princípios e obrigações estão estreitamente alinhados com os estabelecidos no RGPD.

(24) O CEPD congratula-se com o facto de a ANPD ter adotado um Regulamento de Comunicação de Incidente de Segurança vinculativo adicional, que apresenta o conceito de incidente e pormenores para a avaliação da respetiva gravidade (por exemplo, quando se considera que o incidente cria riscos para os titulares dos dados ou afeta significativamente os interesses e direitos fundamentais dos titulares dos dados e, por conseguinte, deve ser comunicado à ANPD e ao titular dos dados), bem como os requisitos de notificação de incidentes[23]. A este respeito, o CEPD observa que, de acordo com o Regulamento de Comunicação de Incidente de Segurança, regra geral, «[a] comunicação de incidente de segurança à ANPD deverá ser realizada pelo [responsável pelo tratamento] no prazo de três dias úteis»[24] e convida a Comissão Europeia a alinhar o seu projeto de decisão (considerando 75) em conformidade[25].

(25) No que diz respeito à notificação de violações de dados, o CEPD assinala que a LGPD afirma que essa notificação (tanto à ANPD como ao titular dos dados) deve incluir, nomeadamente, informações sobre as medidas técnicas e de segurança utilizadas para a proteção de dados pessoais, adotadas antes e depois do incidente, respeitando os segredos comercial e industrial (artigo 6.º, ponto III, e artigo 9.º, ponto II, da LGPD). O CEPD compreende a necessidade de assegurar efetivamente que o direito à privacidade e à proteção de dados

[22] Ver considerando 81 do projeto de decisão.
[23] Ver considerandos 73 a 77 do projeto de decisão.
[24] Ver artigos 6.º e 9.º do Regulamento de Comunicação de Incidente de Segurança.
[25] Ver considerando 75 do projeto de decisão, segundo o qual «[a] comunicação de um incidente de segurança à ANPD e aos titulares dos dados deve ocorrer no prazo de três dias (72 horas) a contar do momento em que o responsável pelo tratamento tomou conhecimento do mesmo».

não afeta negativamente a proteção de outros direitos e convida a Comissão a acompanhar a aplicação dessa limitação, caso as informações sobre o incidente sejam facultadas parcialmente (tendo em conta os segredos comercial e industrial) e o seu impacto nos poderes da ANPD, se for caso disso.

2.3.3 Licitude do tratamento

(26) O CEPD observa que o princípio da licitude e a sua aplicação, conforme previsto na LGPD (artigo 5.º, ponto XII, e artigos 7.º, 8.º e 10.º), está estreitamente alinhado com o princípio consagrado no RGPD (artigo 4.º, n.º 11, e artigos 6.º, 7.º e 9.º) e congratula-se com este alinhamento.

2.3.3.1 Interesse legítimo

(27) Os requisitos do interesse legítimo a utilizar como fundamento jurídico para o tratamento na LGPD (artigo 7.º, ponto IX) estão alinhados com o RGPD [artigo 6.º, n.º 1, alínea f)]. A LGPD salienta igualmente que os direitos e liberdades fundamentais (que incluem o direito à proteção de dados[26]) devem normalmente prevalecer.

(28) O CEPD observa que o artigo 10.º da LGPD enumera as finalidades legítimas para as quais esse fundamento jurídico pode ser utilizado. Uma destas finalidades legítimas consiste em apoiar e promover a atividade do responsável pelo tratamento (artigo 10.º, ponto I, da LGPD).

(29) Embora esta expressão se afigure ampla, o CEPD assinala que as condições para o recurso ao «interesse legítimo» são pormenorizadas no documento *Guia orientativo — Hipóteses legais de tratamento de dados pessoais — Legítimo interesse* («Guia relativo aos interesses legítimos») que a ANPD adotou. O referido guia esclarece que, para que um interesse seja considerado «legítimo», devem ser preenchidas três condições: 1) compatibilidade com o ordenamento jurídico brasileiro; 2) referência a uma situação concreta; e 3) que o tratamento esteja associado a finalidades legítimas, específicas e explícitas[27]. Estas condições são semelhantes a três condições cumulativas para que o tratamento de dados pessoais seja lícito ao abrigo deste fundamento jurídico, especificado pelo TJUE[28], e à sua explicação adicional apresentada pelo Tribunal de Justiça. Além disso, as condições para o «interesse legítimo» especificadas no Guia relativo aos interesses legítimos aproximam-se das condições constantes das diretrizes adotadas pelo CEPD[29]. O CEPD congratula-se com a abordagem adotada pela ANPD no que diz respeito ao interesse legítimo e à sua utilização para o tratamento.

2.4 Direitos das pessoas singulares

(30) O CEPD congratula-se com o facto de a LGPD conferir às pessoas singulares direitos semelhantes aos previstos no RGPD (ambos no capítulo III). Em especial, a LGPD prevê o direito de acesso, o direito de retificação, o direito à portabilidade dos dados, o direito à limitação do tratamento, o direito ao apagamento, o direito à informação, o direito de recusar

[26] Ver o n.º 3 do presente parecer.
[27] Ver considerando 52 do projeto de decisão.
[28] Por exemplo, acórdão do Tribunal de Justiça de 7 de dezembro de 2023, SCHUFA Holding AG, processos apensos C-26/22 e C-64/22, ECLI:EU:C:2023:958, n.ºs 75 a 80.
[29] *Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR — Version 1.0* (não traduzido para português), adotadas em 8 de outubro de 2024.

ou retirar o consentimento, o direito de oposição ao tratamento e o direito de petição (artigos 9.º e 18.º da LGPD).

(31) A LGPD também confere aos titulares dos dados o direito de solicitar a revisão de decisões tomadas exclusivamente com base no tratamento automatizado de dados pessoais que afetem os seus interesses (artigo 20.º da LGPD). O teor do artigo 20.º da LGPD reflete, no essencial, o artigo 22.º do RGPD.

(32) O CEPD observa que, em relação aos direitos dos titulares dos dados, a Lei brasileira de *habeas data* estabelece disposições específicas para conceder o direito de acesso e o direito de retificação num curto prazo (10 e 15 dias, respetivamente) a contar do pedido de uma pessoa singular, e congratula-se com este aspeto.

(33) O CEPD considera que a LGPD estabelece requisitos para os direitos dos titulares dos dados essencialmente equivalentes aos garantidos no RGPD.

2.5 Restrições relativas a transferências ulteriores

(34) O Documento de referência relativo à adequação esclarece que o nível de proteção das pessoas singulares cujos dados pessoais são transferidos ao abrigo de uma decisão de adequação não deve ser comprometido pela transferência ulterior e, por conseguinte, quaisquer transferências ulteriores «só devem ser permitidas se o destinatário seguinte (ou seja, o destinatário da transferência subsequente) também estiver sujeito a normas (incluindo normas contratuais) que garantam um nível de proteção adequado e seguir as instruções pertinentes aquando do tratamento de dados em nome do responsável pelo tratamento dos dados».

(35) Em relação à avaliação da adequação do quadro jurídico e das práticas do Brasil, entende-se por transferência ulterior a transferência de dados pessoais da entidade que atua na qualidade de responsável pelo tratamento, no âmbito territorial da LGPD no Brasil, para a entidade fora deste âmbito.

(36) Os requisitos relativos à transferência ulterior estão estabelecidos no capítulo V da LGPD e a ANPD complementa-os através da adoção do Regulamento Transferência de Dados, que contém as definições de «transferência», «transferência internacional de dados», «importador» e «exportador» e que inclui requisitos pormenorizados aplicáveis às transferências.

(37) O CEPD assinala com agrado que as definições de «transferência» e de «transferência internacional de dados» estão alinhadas com as das Diretrizes 05/2021 do CEPD[30].

(38) De acordo com a LGPD e o Regulamento Transferência de Dados, as transferências ulteriores só podem ter lugar para finalidades legítimas, específicas e explícitas e quando existirem instrumentos ou condições específicos (artigo 33.º da LGPD e artigos 9.º a 33.º do Regulamento Transferência de Dados)[31]. O CEPD congratula-se com o facto de estes instrumentos se aproximarem dos instrumentos de transferência previstos no capítulo V do RGPD. Todavia, o CEPD convida a Comissão Europeia a clarificar, no projeto de decisão, se as transferências só podem ser efetuadas em conformidade com o artigo 33.º, pontos III a IX,

[30] *Diretrizes 05/2021 sobre a interação entre a aplicação do artigo 3.º e as disposições relativas às transferências internacionais nos termos do capítulo V do RGPD*, adotadas em 14 de fevereiro de 2023, n.º 9.
[31] Ver também considerandos 101 a 109 do projeto de decisão.

da LGPD em circunstâncias excecionais, quando as condições previstas no artigo 33.º, pontos I e II, da LGPD não estiverem preenchidas[32].

(39) Todavia, o Regulamento Transferência de Dados especifica que as transferências internacionais de dados pessoais são permitidas quando o titular dos dados tiver dado um consentimento específico e distinto para essa transferência, com informações prévias sobre a natureza internacional da operação prevista, distinguindo-a claramente de outras finalidades. Não é claro se tal requisito implica a obrigação de informar os titulares dos dados sobre os possíveis riscos das transferências internacionais decorrentes da ausência de proteção adequada no país terceiro e da ausência de garantias adequadas (por exemplo, informação de que poderá não existir uma autoridade de controlo e/ou princípios de tratamento de dados e/ou direitos dos titulares dos dados no país terceiro), o que constitui um requisito nos termos do artigo 49.º, n.º 1, alínea a), do RGPD. Para o CEPD, e ao abrigo do RGPD, a prestação destas informações é essencial para permitir que o titular dos dados dê um consentimento esclarecido com pleno conhecimento destes factos específicos da transferência. Assim, o CEPD convida a Comissão Europeia a clarificar, no projeto de decisão, se o titular dos dados é informado sobre os eventuais riscos dessa transferência decorrentes da ausência de proteção adequada no país terceiro e de garantias adequadas.

(40) Além disso, o Regulamento Transferência de Dados prevê que «[o] controlador e o operador deverão adotar medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e da eficácia dessas medidas, de forma compatível com o grau de risco do tratamento e com o mecanismo de transferência internacional utilizado» (artigo 4.º, n.º 2, do Regulamento Transferência de Dados). O CEPD congratula-se com a inclusão desta obrigação. Ao mesmo tempo, seria útil clarificar que a eficácia destas medidas deve ser avaliada de modo a assegurar igualmente que a legislação local do país terceiro em causa não compromete a continuidade da proteção dos titulares de dados cujos dados são transferidos[33]. O CEPD convida a Comissão Europeia a clarificar se este elemento também será tido em conta nos cenários de transferência.

(41) O CEPD congratula-se com a inclusão de um requisito de transparência explícito em relação ao titular dos dados, ou seja, os titulares dos dados têm o direito de receber o instrumento contratual utilizado para a transferência ulterior, bem como a descrição dessa transferência, por exemplo, a duração e a finalidade da transferência, os países de destino, as responsabilidades das partes envolvidas, os direitos dos titulares dos dados e os meios para os exercer (artigo 16.º do Regulamento Transferência de Dados).

(42) Todavia, afigura-se que esse âmbito de aplicação da obrigação de transparência só é relevante quando as transferências são efetuadas com base em cláusulas contratuais-tipo e não quando são utilizados outros instrumentos[34]. Por conseguinte, o CEPD convida a Comissão Europeia a clarificar se são aplicáveis as mesmas obrigações de transparência independentemente do instrumento de transferência utilizado.

[32] O artigo 49.º do RGPD especifica que as derrogações previstas no referido artigo só podem ser utilizadas na falta de uma decisão de adequação nos termos do artigo 45.º, n.º 3, do RGPD, ou de garantias adequadas nos termos do artigo 46.º do RGPD.

[33] Ver acórdão Latombe. Ver também acórdão do Tribunal de Justiça de 16 de julho de 2020, Facebook Ireland e Schrems, processo C-311/18, ECLI:EU:C:2020:559 («acórdão Schrems II»).

[34] Por exemplo, o Regulamento Transferência de Dados inclui requisitos gerais de transparência quando se pretende utilizar regras vinculativas aplicáveis às empresas, em especial a criação e execução de um programa de governação da privacidade que pretenda estabelecer uma relação de confiança com o titular dos dados, através de ações transparentes que assegurem mecanismos de participação do titular dos dados (artigo 25.º, ponto V, do Regulamento Transferência de Dados) e de transparência no que respeita ao exercício dos direitos e do direito de reclamação do titular dos dados (artigo 26.º, ponto VI, do Regulamento Transferência de Dados).

(43) O CEPD observa igualmente que os requisitos relativos ao teor das regras vinculativas aplicáveis às empresas não estão em plena consonância com os requisitos do RGPD, em especial o artigo 47.º, n.º 2, alíneas f) e l), do RGPD. A fim de assegurar que o nível de proteção proporcionado pelo RGPD não é comprometido, o CEPD convida a Comissão Europeia a clarificar, no projeto de decisão, se estes elementos[35] também serão tidos em conta quando for necessário recorrer a este instrumento de transferência para transferências ulteriores de dados pessoais para o Brasil ao abrigo da decisão de adequação.

2.6 Mecanismos processuais e de execução

(44) De acordo com o Documento de referência relativo à adequação[36] e com a jurisprudência pertinente do TJUE[37], um sistema de proteção de dados essencialmente equivalente ao modelo da União Europeia deve prever: i) uma autoridade independente, que deve supervisionar e executar a legislação em matéria de proteção de dados, com poderes para investigar e tomar medidas sem ingerência externa. Os sistemas de proteção de dados devem assegurar ii) que os responsáveis pelo tratamento e os subcontratantes são responsáveis e estão cientes das suas responsabilidades, ao passo que os titulares dos dados são informados dos seus direitos. Devem existir sanções e processos de verificação eficazes para assegurar o cumprimento das regras; iii) que os responsáveis pelo tratamento de dados e os subcontratantes demonstrem a conformidade, através de medidas como avaliações de impacto sobre a proteção de dados, registos das atividades de tratamento e a nomeação de encarregados da proteção de dados. Além disso, iv) o sistema de proteção de dados deve prever apoio e ajuda destinada aos titulares de dados no exercício dos seus direitos e mecanismos de recurso adequados.

(45) Na presente secção, o CEPD centrou a sua avaliação na existência de uma autoridade independente, de um mecanismo de recurso adequado e de sanções eficazes.

2.6.1 Supervisão independente

(46) A LGPD criou a Agência Nacional de Proteção de Dados (ANPD) como autoridade nacional de controlo responsável pelo acompanhamento e aplicação das suas disposições.

(47) O CEPD congratula-se com o facto de ter sido concedido à ANPD o estatuto de «autoridade de natureza especial», uma designação destinada a assegurar a autonomia necessária para exercer plenamente as funções e os poderes jurídicos que a LGPD lhe confere, nomeadamente através da revogação de disposições que subordinam o funcionamento e as operações financeiras da ANPD a autorizações a conceder pelo poder executivo.

(48) Do mesmo modo, o CEPD congratula-se com as alterações introduzidas em 15 de setembro de 2025 no quadro jurídico brasileiro, segundo as quais a ANPD é agora reconhecida como uma **agência reguladora**[38]. Por conseguinte, o CEPD entende que uma das principais alterações é que a ANPD apresentará o seu orçamento diretamente ao Ministério do Planejamento e Orçamento, em vez de ter de o apresentar através do Ministério da Justiça. O orçamento da ANPD continua a constituir-se como uma rubrica separada no orçamento do Estado federal. O CEPD entende que a ANPD já tinha independência em relação ao seu

[35] Responsabilidade e cooperação com a autoridade de controlo [artigo 47.º, n.º 2, alíneas f) e l), do RGPD].
[36] Ver capítulo 3, secção C, do Documento de referência relativo à adequação.
[37] Acórdão do Tribunal de Justiça de 6 de outubro de 2015, Maximillian Schrems/Data Protection Commissioner, processo C-362/14, ECLI:EU:C:2015:650.
[38] Medida provisória n.º 1.317, de 17 de setembro de 2025, disponível em https://www.in.gov.br/en/web/dou/-/medida-provisoria-n-1.317-de-17-de-setembro-de-2025-656784314.

orçamento e financiamento, mas, ao tornar-se uma agência reguladora, o seu processo administrativo é simplificado.

(49) O CEPD congratula-se igualmente com a nova competência da ANPD, que foi recentemente designada como a autoridade responsável pela proteção das crianças em linha[39]. O CEPD toma nota de que, de acordo com o capítulo IX da LGPD, a ANPD está bem equipada com os poderes e missões necessários e disponíveis para assegurar o cumprimento dos direitos em matéria de proteção de dados e promover a sensibilização, como os poderes de investigação e sancionatórios (artigo 55.º-J da LGPD).

(50) Em relação ao pessoal e ao orçamento da ANPD, que desempenha um papel na sua independência, o CEPD assinala com agrado a recente decisão de aumentar o número de pessoal com mais de 200 novos cargos[40].

(51) O CEPD observa que, nos termos do artigo 55.º-C da LGPD, a (atual) ANPD é composta por uma série de organismos[41], incluindo o Conselho Nacional de Proteção de Dados Pessoais e da Privacidade («Conselho»). O CEPD toma nota da sua composição, que inclui também representantes do poder executivo federal, do poder legislativo e do poder judicial[42]. O CEPD assinala igualmente que, nos termos do artigo 58.º-B da LGPD, o Conselho é responsável, nomeadamente, por i) «propor diretrizes estratégicas e fornecer subsídios para a elaboração da Política Nacional de Proteção de Dados Pessoais e da Privacidade e para a atuação da ANPD», e ii) «sugerir ações a serem realizadas pela ANPD».

(52) No que diz respeito, em especial, a estas funções, o CEPD considera importante compreender mais claramente de que modo são aplicadas e em que medida as propostas e recomendações do Conselho influenciam o trabalho da ANPD. Por conseguinte, convida a Comissão Europeia a aprofundar estas funções e a interação entre o Conselho e a ANPD, a fim de avaliar melhor a influência do Conselho nas atividades da ANPD.

2.6.2 Recurso

(53) O CEPD congratula-se com o mecanismo de recurso previsto pela LGPD, que também confere aos titulares dos dados o direito de apresentar uma reclamação à ANPD e de contestar a sua decisão por meio de recurso junto do seu Conselho Diretor. Seguidamente, as pessoas singulares podem recorrer das decisões do Conselho Diretor em tribunal, bem como intentar recurso contra a ANPD por incumprimento das obrigações que lhe incumbem por força da LGPD. Com base no projeto de decisão, não fica clara a diferença entre o ato de recurso e o instrumento de recurso. O CEPD convida a Comissão a clarificar melhor o funcionamento destas duas vias, nomeadamente se o recurso se limita apenas à recusa de tratamento de uma reclamação ou a uma rejeição quanto ao mérito de uma reclamação.

(54) Do mesmo modo, o CEPD congratula-se com a disposição relativa ao direito a indemnização por danos morais ou materiais, bem como à tutela coletiva (artigo 22.º da LGPD).

---

[39] Lei n.º 15.211, de 17 de setembro de 2025, sobre a proteção de crianças e adolescentes em ambientes digitais, disponível em https://www.in.gov.br/web/dou/-/lei-n-15.211-de-17-de-setembro-de-2025-656579619.
[40] https://www.in.gov.br/en/web/dou/-/medida-provisoria-n-1.317-de-17-de-setembro-de-2025-656784314.
[41] Nos termos do artigo 55.º-C da LGPD, a ANPD é composta: pelo Conselho Diretor, órgão máximo de direção; pelo Conselho Nacional de Proteção de Dados Pessoais e da Privacidade; pela Corregedoria [o conselho de disciplina]; IV — pela Ouvidoria [o gabinete do provedor de justiça]; VI — pelo órgão de assessoramento jurídico próprio e VI — pelas unidades administrativas e unidades especializadas necessárias para a aplicação das disposições da LGPD. Ver também considerandos 126 a 130 do projeto de decisão.
[42] Ver também o considerando 132 do projeto de decisão e o artigo 55.º-C da LGPD.

2.6.3 Sanções

(55) O CEPD recorda que a existência de sanções eficazes e dissuasivas pode desempenhar um papel importante na garantia do respeito das regras em matéria de proteção de dados, pois é um sinal do elevado grau de responsabilização e de sensibilização que o sistema garante. O CEPD congratula-se com os poderes de correção de que a ANPD dispõe, que foram exercidos em várias ocasiões[43] e que incluem uma série de medidas, como uma advertência, multas até dois por cento (2 %) das receitas brutas da entidade jurídica privada envolvida, multas diárias, o bloqueio dos dados pessoais relacionados com a infração até à sua regularização, a suspensão temporária das atividades de tratamento de dados pertinentes e o apagamento dos dados pessoais em causa (artigo 52.º da LGPD)[44]. O CEPD convida a Comissão a acompanhar a sua aplicação coerente, em especial no que diz respeito às sanções.

(56) O CEPD assinala com agrado que a ANPD emitiu um Regulamento relativo às sanções (vinculativo). O referido regulamento classifica as sanções em diferentes níveis, utilizando fatores objetivos como o tipo e o volume de dados sujeitos a tratamento ou o impacto dos direitos dos titulares dos dados, e prevê uma metodologia de cálculo das multas, que está em conformidade com os requisitos constantes do artigo 83.º do RGPD.

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

(57) Nos termos do artigo 45.º, n.º 2, do RGPD, a avaliação das limitações e garantias previstas na legislação brasileira no que diz respeito ao acesso e utilização subsequente pelas autoridades públicas brasileiras de dados pessoais transferidos para responsáveis pelo tratamento e subcontratantes no Brasil para efeitos de aplicação do direito penal e de segurança nacional («acesso governamental») é um elemento importante do teste de «equivalência essencial», conforme interpretação do TJUE.

(58) O CEPD assinala com agrado a atenção específica que a Comissão prestou a este aspeto no projeto de decisão e as informações factuais que facultou sobre o mesmo[45]. Por conseguinte, o CEPD opta por não reproduzir no presente parecer a maioria das conclusões e análises factuais. Em vez disso, avalia a ingerência do sistema brasileiro no que se refere ao acesso governamental para efeitos de aplicação da lei e de segurança nacional com base nos quatro elementos identificados pelo CEPD nas garantias essenciais europeias relativas às medidas de vigilância, adotadas em 10 de novembro de 2020[46]:

- garantia A — regras jurídicas claras, precisas e acessíveis,

[43] Ver ANPD, registo de sanções: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/decisoes-em-processos-sancionadores-1/decisoes-em-processos-sancionadores?_authenticator=7951f0a70d3d125fd05e11a1e544b72d2c61f304.
[44] «Estas sanções podem ser impostas a entidades públicas ou privadas, com exceção das multas e multas diárias que não podem ser impostas a entidades públicas» (considerando 135 do projeto de decisão).
[45] Ver considerandos 152 a 217 do projeto de decisão.
[46] Recomendações 02/2020 sobre as garantias essenciais europeias relativas às medidas de vigilância.

- garantia B — necessidade e proporcionalidade em relação aos objetivos legítimos prosseguidos,
- garantia C — mecanismo de supervisão independente,
- garantia D — vias de recurso eficazes e mecanismos de recurso à disposição das pessoas singulares.

3.1 Acesso e utilização pelas autoridades públicas brasileiras para efeitos de aplicação do direito penal

3.1.1 Quadro jurídico no domínio da aplicação do direito penal

(59) O CEPD assinala que o acesso a dados pessoais pelas autoridades de aplicação da lei e a utilização subsequente desses dados[47] são regulados por um sistema de atos jurídicos de natureza jurídica diferente. A proteção de dados e a privacidade, incluindo o sigilo da correspondência e das comunicações, estão consagradas no artigo 5.º da Constituição como direitos fundamentais. O CEPD congratula-se, em especial, com o facto de o âmbito da proteção desses direitos, à semelhança do que sucede na UE, não se limitar apenas aos cidadãos brasileiros, mas abranger também estrangeiros residentes no Brasil ou não[48].

(60) Seguidamente, existem várias leis setoriais especializadas que regem o eventual acesso a dados pessoais para efeitos de aplicação do direito penal. No que respeita ao acesso aos dados transferidos da UE para o Brasil, são de especial pertinência o Código de Processo Penal, a Lei relativa à interceção de comunicações telefónicas, o Marco Civil da Internet, a Lei relativa ao sigilo das operações de instituições financeiras, a Lei relativa às organizações criminosas e investigações criminais, entre outros. O CEPD assinala que estes atos jurídicos estão acessíveis ao público e podem ser considerados suficientemente claros para dar aos titulares dos dados uma indicação sobre as circunstâncias e as condições em que as autoridades públicas estão habilitadas a aceder aos seus dados[49].

(61) Outra importante fonte de direito no Brasil é a jurisprudência do Supremo Tribunal Federal do Brasil, que se afigura aplicar uma interpretação ampla do âmbito dos direitos à privacidade e à proteção de dados[50], bem como a jurisprudência da Corte Interamericana de Direitos Humanos, responsável pela interpretação e aplicação da Convenção Americana sobre Direitos Humanos, que o Brasil ratificou em 1992[51].

(62) O CEPD observa que o âmbito de aplicabilidade da LGPD em caso de tratamento de dados pessoais para efeitos de aplicação do direito penal é parcial, o que pode conduzir a insegurança jurídica.

(63) Conforme a Comissão reconheceu no projeto de decisão, a LGPD não se aplica ao tratamento de dados realizado para fins *exclusivos* de segurança pública, defesa nacional, segurança do Estado ou investigação e repressão de infrações penais[52]. Nos termos do artigo 4.º, pontos I e III, da LGPD, o tratamento de dados nestes domínios será regido por legislação específica, que deve abranger os princípios e os direitos dos titulares dos dados

[47] Ver a lista de autoridades constante do considerando 165 do projeto de decisão.
[48] Ver considerandos 8 e 9 do projeto de decisão.
[49] Ver acórdão do TEDH no processo Zakharov, n.º 229.
[50] Ver Supremo Tribunal Federal, Decisão relativa à ADI 6649, de 15 de setembro de 2022.
[51] Ver considerando 10 do projeto de decisão.
[52] Ver considerandos 30 e 31 do projeto de decisão.

enunciados na LGPD. Tanto quanto é do conhecimento do CEPD, confirmado pela Comissão, o Brasil ainda não adotou legislação específica relativa ao tratamento de dados pessoais no domínio da justiça penal e da aplicação da lei (por exemplo, semelhante à Diretiva Proteção de Dados na Aplicação da Lei da UE[53]).

(64) O CEPD assinala com agrado que, na sua jurisprudência[54], o Supremo Tribunal Federal do Brasil interpretou a LGPD de uma forma que alargou a sua aplicabilidade parcial ao tratamento de dados pessoais para efeitos de investigações criminais e manutenção da ordem pública.

(65) O CEPD congratula-se com o facto de a autoridade de controlo do Brasil, a ANPD, apoiar plenamente esta interpretação e considerar que «a inexistência de legislação específica não confere ampla e irrestrita autorização aos órgãos de segurança para tratarem dados pessoais dos cidadãos para finalidades exclusivas de segurança pública e atividades de investigação e repressão de infrações penais sem quaisquer tipos de limites»[55]. Ao mesmo tempo, o CEPD assinala que, nos termos do artigo 4.º, ponto III, n.º 3, da LGPD, para algum tratamento específico de dados efetuado exclusivamente para efeitos de aplicação do direito penal, a ANPD afigura-se ter, neste momento, principalmente um papel consultivo junto das autoridades responsáveis pela aplicação da lei.

(66) O CEPD convida a Comissão a avaliar e clarificar mais aprofundadamente, no projeto de decisão, a aplicabilidade da LGPD em caso de tratamento de dados pessoais para efeitos de aplicação do direito penal, incluindo os poderes da ANPD, bem como a ter cuidadosamente em conta qualquer evolução pertinente a este respeito no seu futuro acompanhamento (ver também a secção sobre supervisão e recurso).

3.1.2 Necessidade e proporcionalidade

(67) O CEPD assinala com agrado que, regra geral, o acesso a dados de comunicações, tanto ao teor como aos metadados, bem como a outras categorias de informações confidenciais protegidas, como os dados bancários e fiscais, exige uma autorização judicial prévia.

(68) No que diz respeito ao acesso a dados de comunicações, o CEPD congratula-se com o facto de, nos termos da Lei relativa à interceção de comunicações telefónicas e da jurisprudência do Supremo Tribunal Federal, essa medida ser considerada excecional e estar sujeita a condições rigorosas destinadas a assegurar a sua necessidade e proporcionalidade[56]. Além disso, como medida preventiva contra eventuais abusos, a legislação brasileira prevê que a interceção de comunicações sem autorização judicial ou para fins não autorizados por lei constitui um crime punível com até quatro anos de prisão[57].

(69) A aplicação rigorosa das garantias para o acesso a dados de comunicações é especialmente pertinente, tendo em conta a existência, no Brasil, de uma obrigação geral de conservação de dados para os prestadores de serviços de ligação à Internet e de aplicações em linha de

[53] Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho (JO L 119 de 4.5.2016, p. 89).
[54] Ver Supremo Tribunal Federal, Decisão relativa à ADI 6649, de 15 de setembro de 2022.
[55] Ver ANPD, Nota Técnica n.º 29/2024/FIS/CGF/ANPD, dirigida ao Ministério da Justiça e Segurança Pública, ponto 5.4.1.29, disponível em: SEI/ANPD - 0132350 - Nota Técnica.
[56] Ver considerandos 169 e 170 do projeto de decisão.
[57] *Ibidem*.

conservarem os registos de ligação durante um ano[58]. Embora assinale com agrado que o acesso aos dados conservados só é possível sob reserva de uma autorização judicial[59], o CEPD recorda a abordagem rigorosa e as restrições à conservação geral e indiscriminada de metadados de comunicações na UE[60] e toma nota positiva das informações adicionais facultadas pela Comissão em relação à ausência de conservação de dados em massa no país. Por conseguinte, o CEPD incentiva a Comissão a prestar especial atenção ao regime jurídico e às práticas no Brasil no que diz respeito ao acesso a dados de comunicações durante o acompanhamento e a revisão do projeto de decisão.

(70) O CEPD assinala com agrado que se aplicam garantias semelhantes também no que diz respeito ao acesso das autoridades responsáveis pela aplicação da lei a dados fiscais e bancários, ou seja, à exigência de autorização judicial prévia, permitida apenas no caso de crimes graves, existência de sanções penais em caso de abuso, etc.

(71) De acordo com o projeto de decisão, existe uma exceção ao requisito geral de autorização judicial prévia para o acesso das autoridades responsáveis pela aplicação da lei a determinadas categorias de dados pessoais[61]. Nos termos dos artigos 15.º e 16.º da Lei relativa às organizações criminosas e investigações criminais, um chefe da polícia e o Ministério Público podem aceder, sem autorização judicial, aos dados de registo de uma pessoa investigada sobre: «a qualificação pessoal, a filiação e o endereço mantidos pela Justiça Eleitoral, empresas telefônicas, instituições financeiras, provedores de internet e administradoras de cartão de crédito»[62]. Na mesma ordem de ideias, as empresas de transportes permitirão, durante um período de cinco anos, o acesso direto e permanente de um juiz, do Ministério Público ou de um chefe da polícia às bases de dados de reservas e registos de viagem[63].

(72) O CEPD assinala que o âmbito de aplicação da Lei relativa às organizações criminosas e investigações criminais se limita à investigação e sanção de grupos de criminalidade organizada e de organizações terroristas, o que representa um risco significativo para os cidadãos e a sociedade e, por conseguinte, é suscetível de justificar uma ingerência mais grave nos direitos fundamentais à privacidade e à proteção de dados[64]. Ao mesmo tempo, o CEPD considera que as informações sobre estas exceções constantes do considerando 164 do projeto de decisão são muito gerais e não estão completas. Em especial, das informações constantes do projeto de decisão não fica claro se, nesse caso, o acesso a dados pessoais está sujeito a um controlo jurisdicional *ex post* da necessidade e da proporcionalidade.

(73) Tendo em conta o que precede, o CEPD convida a Comissão a clarificar e explicar mais pormenorizadamente, no projeto de decisão, o âmbito e a natureza dos casos em que o acesso aos dados pelas autoridades responsáveis pela aplicação da lei não exige autorização judicial, bem como as garantias aplicáveis constantes da legislação brasileira. O CEPD

[58] Ver considerando 173 do projeto de decisão.
[59] *Ibidem*.
[60] Para mais informações sobre a conservação de dados, ver o documento *Statement 5/2024 on the Recommendations of the High Level Group on Access to Data for Effective Law Enforcement* (não traduzido para português), disponível em https://www.edpb.europa.eu/system/files/2024-11/edpb_statement_20241104_ontherecommendationsofthehlg_en.pdf.
[61] Ver considerando 164 do projeto de decisão.
[62] Ver artigo 15.º da Lei relativa às organizações criminosas e investigações criminais.
[63] Ver artigo 16.º da Lei relativa às organizações criminosas e investigações criminais.
[64] Ver acórdão do Tribunal de Justiça de 6 de outubro de 2020, La Quadrature du Net e o., processos apensos C-511/18 e C-512/18, ECLI:EU:C:2020:791, n.os 95 a 98; acórdão do Tribunal de Justiça de 2 de outubro de 2018, Ministerio Fiscal, C-207/16, ECLI:EU:C:2018:788, n.os 54, 57 e 60; acórdão do Tribunal de Justiça de 2 de março de 2021, Prokuratuur (Condições de acesso aos dados relativos às comunicações eletrónicas), C-746/18, ECLI:EU:C:2021:152, n.º 35.

considera igualmente que a Comissão, durante o acompanhamento do projeto de decisão, deve prestar especial atenção à aplicação destas exceções ao abrigo da legislação brasileira.

3.1.3 Utilização posterior de dados e transferências ulteriores

(74) O CEPD recorda que o nível de proteção concedido aos dados pessoais transferidos da UE/EEE para o Brasil não deve ser comprometido pela utilização posterior ou partilha dos dados com destinatários no Brasil ou num país terceiro, ou seja, as transferências ulteriores só devem ser permitidas se for assegurado um nível de proteção essencialmente equivalente ao previsto no direito da UE.

(75) A este respeito, o CEPD assinala com agrado que o Supremo Tribunal Federal do Brasil tenha decidido que a partilha de dados pessoais entre organismos públicos (incluindo quando partilhados entre os serviços responsáveis pela aplicação da lei e os serviços de inteligência) pressupõe: 1) a definição de uma finalidade legítima, específica e explícita para o tratamento de dados; 2) a compatibilidade do tratamento com as finalidades informadas; 3) a limitação da partilha ao mínimo necessário para cumprir a finalidade informada; bem como o cumprimento integral dos requisitos, garantias e procedimentos previstos na LGPD, na medida em que sejam compatíveis com o setor público[65].

(76) Não obstante esta importante decisão da mais alta instância jurisdicional do Brasil, dada a complexidade já mencionada, o âmbito exato e as modalidades de aplicação da LGPD às autoridades responsáveis pela aplicação da lei, o CEPD convida a Comissão a acompanhar de perto a evolução e as práticas neste domínio.

(77) No que diz respeito à transferência ulterior de dados pessoais para autoridades responsáveis pela aplicação do direito penal em países terceiros, o projeto de decisão remete para o artigo 33.º, ponto III, da LGPD, que estabelece que a transferência internacional de dados pode ter lugar quando «for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional»[66]. O CEPD considera esta explicação demasiado genérica e convida a Comissão a aprofundar, no projeto de decisão, as condições e garantias que regem as transferências ulteriores.

3.1.4 Supervisão e recurso

(78) O CEPD recorda que qualquer ingerência no direito à privacidade e à proteção dos dados deve ser sujeita a um sistema de supervisão eficaz, independente e imparcial que deve ser fornecido por um juiz ou por outro organismo independente (por exemplo, uma autoridade administrativa ou um órgão parlamentar)[67].

(79) Assinala igualmente que, no quadro brasileiro, conforme descrito pela Comissão, as atividades das autoridades responsáveis pela aplicação do direito penal são supervisionadas por diferentes organismos: i) o poder judicial, ii) a ANPD e iii) o Ministério Público.

[65] Ver considerando 187 do projeto de decisão.
[66] *Ibidem*.
[67] Recomendações 02/2020 sobre as garantias essenciais europeias relativas às medidas de vigilância, adotadas em 10 de novembro de 2020, ver página 12, https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_pt.pdf.

(80) O controlo judicial, conforme explicado *supra*, na secção «Necessidade e proporcionalidade»[68], aplica-se à recolha de dados pessoais e ao acesso aos mesmos, nomeadamente sob a forma de revisão e autorização *ex ante*.

(81) No que diz respeito ao papel da ANPD, conforme já explicado na secção 3.1.1 do presente parecer, o projeto de decisão de adequação recorda que, nos termos do artigo 4.º, ponto III, da LGPD, esta lei não se aplica ao tratamento de dados pessoais realizado para fins *exclusivos* de i) segurança pública, ii) defesa nacional, iii) segurança do Estado e iv) investigação e repressão de infrações penais. Além disso, o artigo 4.º, n.º 1, estabelece que esse tratamento será regido por legislação específica, que deverá, nomeadamente, abranger os princípios gerais de proteção e os direitos do titular dos dados previstos na LGPD. O n.º 3 do mesmo artigo reconhece um papel consultivo à ANPD em relação às exceções previstas no ponto III, quando realizadas exclusivamente para esses fins, nomeadamente os poderes da ANPD para emitir pareceres técnicos e recomendações, bem como para solicitar AIPD aos responsáveis pelo tratamento competentes.

(82) No seu projeto de decisão[69], a Comissão remete para uma decisão importante, datada de 15 de setembro de 2022, do Supremo Tribunal Federal, que indica a aplicabilidade dos princípios gerais de proteção de dados e dos direitos dos titulares dos dados ao tratamento de dados pessoais pelo Estado para a prestação de serviços públicos. A referida decisão centra-se na «partilha de dados pessoais» entre organismos e entidades da administração pública e em atividades de inteligência, bem como no «acesso de agências e entidades governamentais» ao Registo Base dos Cidadãos. Em relação ao papel de execução da ANPD, o CEPD entende, com base em informações adicionais facultadas pela Comissão, que a ANPD já exerceu esse papel sobre a polícia, bem como sobre o Ministério da Justiça e Segurança Pública. Tal foi feito com base na jurisprudência que, ao alargar a aplicabilidade parcial dos princípios gerais e dos direitos dos titulares dos dados ao tratamento efetuado para efeitos de aplicação do direito penal, torna a ANPD responsável pela supervisão e aplicação da lei igualmente neste domínio.

(83) Tendo em conta o que precede, o CEPD convida a Comissão a aprofundar o papel de aplicação da lei que a ANPD desempenha, nomeadamente no que diz respeito aos fundamentos jurídicos pertinentes e aos seus poderes de investigação e correção em relação às autoridades responsáveis pela aplicação da lei, e a acompanhar de perto a evolução da situação neste domínio.

(84) Por último, o CEPD observa que o Ministério Público possui uma competência mais ampla do que a supervisão das regras em matéria de proteção de dados e privacidade e a imposição de sanções por violações dos direitos fundamentais. Por exemplo, conforme já explicado na secção 3.1 do presente parecer, nos termos da Lei relativa às organizações criminosas e investigações criminais, o Ministério Público é uma das autoridades que podem aceder, sem autorização judicial, aos dados de registo de uma pessoa investigada. Por conseguinte, o CEPD convida a Comissão a aprofundar e explicar, no projeto de decisão, o papel e os poderes do Ministério Público em relação à supervisão do tratamento de dados pessoais pelas autoridades brasileiras responsáveis pela aplicação da lei.

(85) No que diz respeito às vias de recurso, o CEPD assinala com agrado que os mecanismos jurídicos descritos na primeira parte do presente parecer e, em especial, as vias de recurso judiciais à disposição das pessoas para fazerem valer os seus direitos à proteção de dados

[68] Ver secção 3.1.2 *supra*.
[69] Ver considerando 187 do projeto de decisão.

e à privacidade também se aplicam às atividades dos organismos responsáveis pela aplicação do direito penal.

3.2 Acesso e utilização pelas autoridades públicas brasileiras para efeitos de segurança nacional

3.2.1 Âmbito de aplicação da isenção do artigo 4.º, ponto III, da LGPD e sua aplicabilidade a infrações penais contra a segurança do Estado

(86) Conforme introduzido pela Comissão, o artigo 4.º, ponto III, da LGPD isenta a «segurança do Estado» da aplicação da LGPD ao proceder ao tratamento de dados pessoais, juntamente com a segurança pública, a defesa nacional e as atividades de investigação e repressão de infrações penais.

(87) O CEPD assinala que a legislação brasileira em matéria de segurança nacional, conforme estabelecida na Lei n.º 14.197, de 1 de setembro de 2021, que altera o Código Penal e revoga a Lei de Segurança Nacional de 1983[70], exprime o conceito brasileiro de segurança nacional com base numa lista exaustiva de crimes[71] que abrangem diferentes ameaças à integridade do Estado brasileiro enquanto instituição [soberania nacional, espionagem (artigo 350.º-K), crimes contra as instituições democráticas (artigo 359.º-L), entre outros). As normas constantes da Lei n.º 14.197 foram estabelecidas como parte integrante do Código Penal brasileiro.

(88) Dito isto, o CEPD espera que o tratamento de dados realizado pelas autoridades brasileiras para a repressão das infrações previstas na Lei n.º 14.197 seja regido pelo regime aplicável ao acesso e utilização das autoridades brasileiras para efeitos de aplicação do direito penal, conforme descrito no capítulo 3.2 do projeto de decisão, respondendo assim às mesmas considerações em matéria de proteção de dados que as enunciadas no capítulo 3.1 do presente parecer. Por conseguinte, o CEPD solicita à Comissão que clarifique, no projeto de decisão, se o tratamento de dados relacionado com a repressão dos crimes enumerados na Lei n.º 14.197 é efetivamente regido pelo regime de proteção de dados aplicável às atividades de aplicação da lei, ou por outro regime. Se este último for o caso, o CEPD convida a Comissão a explicar melhor as regras em matéria de proteção de dados aplicáveis à ação penal contra estes crimes para efeitos de segurança nacional.

3.2.2 Quadro jurídico para a segurança nacional

(89) O quadro jurídico codificado no qual o projeto de decisão baseia as suas conclusões no respetivo capítulo sobre o acesso governamental para «efeitos de segurança nacional» é constituído pela Lei n.º 14.197 de 2021, pela Lei n.º 9.883, de 7 de dezembro de 1999, que cria o Sistema Brasileiro de Inteligência, e pelo Decreto n.º 4.376 conexo de 2002. Os dois últimos atos legislativos mencionados criaram o Sistema Brasileiro de Inteligência (SISBIN) e estabeleceram o seu funcionamento. Seguiu-se o Decreto Presidencial n.º 8.793[72], de 2016, que define a Política Nacional de Inteligência (PNI), bem como a LGPD, em 2018.

[70] Lei n.º 14.197, de 1 de setembro de 2021, disponível em https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14197.htm (2.10.2026).
[71] Ver considerando 200 do projeto de decisão.
[72] Ver considerando 199 do projeto de decisão.

(90) O Decreto Presidencial n.º 8.793 de 2016 descreve o objeto, os objetivos e os limites da PNI. As atividades ao abrigo do referido decreto visam produzir e divulgar às autoridades competentes conhecimentos relacionados com factos e situações que ocorram dentro ou fora do território nacional, com influência imediata ou potencial no processo decisório, na ação governamental e na segurança da sociedade e da inteligência do Estado. Nestas circunstâncias, «inteligência» refere-se ao conjunto das informações — e dos dados — necessárias e tratadas para apoiar o processo decisório do poder executivo neste domínio.

(91) De acordo com o fundamento jurídico do SISBIN, conforme apresentado pela Comissão, o SISBIN e as suas entidades foram criados como sendo o mecanismo central para a aplicação da PNI e, como tal, são responsáveis pela realização de atividades relacionadas com a segurança nacional, bem como com a segurança pública e a proteção das instituições democráticas. Para o efeito, o SISBIN proporciona o intercâmbio de conhecimentos e o planeamento integrado das atividades[73]. Consequentemente, o conceito de segurança nacional no Brasil à luz das atividades do SISBIN afigura-se não se limitar unicamente aos crimes codificados na Lei n.º 14.197, podendo ser considerado parte integrante de um conceito mais amplo de inteligência nacional.

(92) Inicialmente, quando foi criado, o SISBIN era composto por 18 entidades federais, entre as quais 13 ministérios, e foi posteriormente alargado a 48 agências designadas ao abrigo do Decreto n.º 11.693, de 6 de setembro de 2023, relativo à organização e ao funcionamento do SISBIN[74]. O CEPD assinala que a cooperação no âmbito do SISBIN integra entidades para além das instituições de segurança clássicas, como o Ministério da Ciência (artigo 4.º, ponto IV), da Agricultura (artigo 4.º, ponto XV) e da Energia (artigo 4.º, ponto XVIII) e o procurador-geral federal (artigo 4.º, ponto XIX).

(93) Enquanto o Decreto n.º 4.376 de 2002 exigia que o Conselho Consultivo do Sistema Brasileiro de Inteligência propusesse normas e procedimentos gerais para o intercâmbio de «conhecimentos e comunicações» no âmbito do SISBIN[75], o Decreto n.º 11.693 de 2023 refere, no Órgão Central do SISBIN, a disponibilização de ferramentas técnicas[76] para a partilha de dados, informações e conhecimentos, bem como descreve a partilha e utilização de dados obtidos pelas entidades do SISBIN. Todavia, o projeto de decisão da Comissão não faculta mais informações sobre essas regras ou normas jurídicas emitidas pelo Órgão Central, por exemplo quando as entidades do SISBIN partilham dados pessoais entre si.

(94) Além disso, afigura-se existirem diferenças nos conceitos de sensibilidade da informação, uma vez que, nos termos da legislação pertinente que rege as atividades da SISBIN, a sensibilidade está relacionada com o grau de confidencialidade concedido a uma informação[77] e com a limitação da finalidade em comparação com os princípios gerais do RGPD[78].

(95) Conforme explicado *supra*, o artigo 4.º, ponto III, alíneas a) a c), da LGPD, codificado apenas após a criação do SISBIN e a definição de uma Política Nacional de Inteligência, isenta da

[73] O Decreto Presidencial n.º 8.793, secção 5, designa o SISBIN e os órgãos nele integrados, o intercâmbio de conhecimentos no âmbito do SISBIN e o planeamento integrado da cooperação entre os membros do SISBIN como instrumentos para a realização da PNI.
[74] Ver considerando 202 do projeto de decisão.
[75] Ver artigo 7.º, ponto II, do Decreto n.º 4.376.
[76] Ver artigo 10.º, ponto XI, disponível em https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/d11693.htm (26.9.2025).
[77] Ver Decreto n.º 8.793 de 2016, Decreto n.º 11.693 e considerando 204 do projeto de decisão.
[78] Ver artigo 6.º, ponto I, da LGPD, que refere finalidades legítimas e específicas, ao passo que o RGPD exige finalidades lícitas e específicas.

aplicação da LGPD as atividades de tratamento de dados realizadas exclusivamente para fins de segurança pública, defesa nacional e segurança do Estado, com exceção dos princípios gerais estabelecidos em matéria de proteção de dados.

(96) Tal como a Comissão sublinhou no projeto de decisão, o quadro geral da Constituição brasileira, bem como a participação do Brasil na Corte Interamericana de Direitos Humanos, dizem respeito ao quadro jurídico do acesso governamental para efeitos de inteligência nacional. O CEPD reconhece igualmente que as decisões do Supremo Tribunal Federal brasileiro também desempenharam um papel importante na definição do panorama jurídico[79]. Até à data, os acórdãos do Supremo Tribunal serviram de apoio conciso e pertinente ao desenvolvimento da proteção de dados pessoais, em conformidade com a Constituição brasileira. Ao mesmo tempo, importa salientar que os acórdãos do Supremo Tribunal não especificam nem estabelecem regras gerais e abstratas de proteção de dados para o tratamento de dados pessoais, mas interpretam as disposições e os princípios da Constituição e da LGPD.

(97) O CEPD está ciente de que é concedida aos Estados uma ampla margem de apreciação na definição de questões de segurança nacional, o que permite, subsequentemente, isenções no domínio da segurança nacional aquando do tratamento de dados pessoais. Neste contexto, o CEPD recorda a definição dada pelo Tribunal Europeu dos Direitos Humanos, segundo a qual as ameaças à segurança nacional devem ser distinguidas pela sua natureza, gravidade e circunstâncias específicas dos riscos gerais para a segurança pública ou dos crimes graves[80].

(98) O CEPD entende que os dados tratados pelas entidades do SISBIN só beneficiam da isenção prevista no artigo 4.º, ponto III, da LGPD quando o tratamento é realizado para fins *exclusivos* de segurança pública, defesa nacional e segurança do Estado. Tal afigura-se aplicar-se especificamente às atividades do Órgão Central do SISBIN, a Agência Brasileira de Inteligência (ABIN). Por conseguinte, a menos que uma entidade do SISBIN atue em nome da ABIN para um destes fins, a LGPD é plenamente aplicável.

(99) O CEPD insta a Comissão a confirmar este entendimento e a descrever e explicar de forma mais precisa, no projeto de decisão, as linhas gerais do conceito de segurança nacional ao abrigo da legislação brasileira, em especial no que diz respeito à recolha e partilha de dados entre e por entidades em nome das atividades do SISBIN e no que diz respeito à execução da PNI. Neste contexto, o CEPD convida a Comissão a clarificar também de que forma as isenções da LGPD para efeitos de segurança nacional se relacionam com a isenção para a segurança nacional ao abrigo do RGPD.

3.2.3 Transferências ulteriores e acordos internacionais

(100) O artigo 33.º da LGPD define as condições prévias para a transferência internacional de dados. O artigo 33.º, pontos I e II, da LGPD estabelece requisitos semelhantes para uma decisão de adequação ou requisitos para garantias adicionais ao abrigo do RGPD. Estes requisitos são dispensados no artigo 33.º, pontos III, VI e VII, da LGPD, que trata dos casos de «cooperação jurídica internacional entre órgãos públicos de inteligência», de transferências que respondem a um «compromisso assumido em acordo de cooperação internacional» e de transferências necessárias «para a execução de política pública ou atribuição legal do serviço público», ou seja, a segurança nacional e a inteligência nacional.

[79] Ver considerando 203 do projeto de decisão.
[80] TEDH, Big Brother Watch e outros/Reino Unido, 25 de maio de 2021, n.º 350.

Esta decisão afigura-se estar em conformidade com o conceito constante do artigo 4.º, ponto III, da LGPD, que limita a aplicação da LGPD apenas aos seus princípios em matéria de segurança pública, defesa nacional e segurança do Estado. Assim, poder-se-ia considerar que as transferências ulteriores para efeitos de inteligência nacional devem ser realizadas em conformidade com os princípios gerais de proteção de dados da LGPD, estando igualmente sujeitas às disposições em matéria de cooperação internacional previstas nos atos jurídicos que criam o PNI e o SISBIN.

(101) Dito isto, o CEPD reconhece que o Brasil poderá necessitar de transmitir dados pessoais a serviços de inteligência estrangeiros, e poderá efetivamente transmiti-los, para efeitos de cooperação ou de execução da PNI, de acordo com o objetivo de prevenir e identificar ameaças com base no conceito integrado de segurança referido *supra*.

(102) Conforme referido anteriormente, a Comissão salienta a aplicabilidade do quadro geral da Constituição brasileira e a garantia de *Habeas Data* para a proteção de dados pessoais no âmbito do SISBIN, que também se aplicam às transferências ulteriores para efeitos de segurança nacional. O CEPD convida a Comissão a clarificar melhor o fundamento jurídico e as garantias e condições em matéria de proteção de dados que a ABIN e os outros membros do SISBIN são obrigados a ter em conta antes de divulgarem dados pessoais a parceiros estrangeiros para efeitos de inteligência nacional.

(103) O CEPD observa igualmente que a Comissão não integrou na sua avaliação da adequação considerações sobre a existência de acordos internacionais celebrados entre o Brasil e países terceiros ou organizações internacionais. Uma vez que a LGPD não prevê legislação vinculativa para além dos princípios gerais de proteção de dados, esses acordos podem conter disposições específicas para a transferência internacional de dados pessoais na posse da ABIN ou de outros membros do SISBIN para países terceiros. O CEPD considera que a celebração de acordos bilaterais ou multilaterais com países terceiros para efeitos de inteligência nacional é suscetível de afetar o quadro jurídico em matéria de proteção de dados aplicável.

(104) Por conseguinte, o CEPD convida a Comissão a esclarecer se esses acordos internacionais para efeitos de inteligência nacional existem e a avaliar o seu potencial impacto no nível de proteção concedido aos dados pessoais transferidos do EEE para o Brasil em relação ao quadro jurídico avaliado inicialmente para o tratamento de dados para efeitos de inteligência nacional.

3.2.4 Supervisão e recurso

(105) O projeto de decisão de adequação apresenta diferentes organismos para supervisionar as atividades das autoridades nacionais de segurança brasileiras, nomeadamente i) o poder executivo, ii) o poder legislativo, iii) a ANPD e iv) o poder judicial. Em relação à ANPD, o CEPD recorda a consideração e as conclusões apresentadas na secção 3.1.4 do presente parecer, que também se mantêm válidas neste contexto.

(106) De acordo com o projeto de decisão, a Câmara de Relações Exteriores e Defesa Nacional do Conselho de Governo é responsável pela supervisão da aplicação da Política Nacional de Inteligência e o Gabinete de Segurança Institucional é responsável pela coordenação da atividade dos serviços de inteligência federais. O CEPD assinala que este controlo se refere apenas à garantia de que o sistema de inteligência alcance os seus objetivos e à sua aplicação, mas não inclui quaisquer poderes de investigação ou sanção, e não abrange o tratamento efetivo de dados pessoais.

(107) Com efeito, cabe à Comissão Mista de Controle das Atividades de Inteligência (CCAI) (poder legislativo) exercer controlo em relação às atividades de inteligência, englobando a sua legitimidade e eficácia. O CEPD congratula-se com o facto de a estrutura e os poderes da CCAI terem sido reforçados, aumentando a transparência em relação às suas atividades e permitindo ao organismo exercer um controlo adequado, como a realização de análises, auditorias e controlos *post hoc* das operações em curso. O CEPD assinala igualmente com agrado que a CCAI pode tratar de reclamações de titulares de dados no âmbito da sua competência para investigar reclamações sobre violações de garantias e direitos fundamentais.

(108) A competência do poder judicial para conhecer de processos intentados por cidadãos contra autoridades públicas é um aspeto positivo, em especial porque permite o controlo judicial das atividades realizadas em nome da segurança nacional, garantindo o respeito, entre outros, dos direitos constitucionais (incluindo o direito à proteção de dados) e da LGPD. O CEPD assinala com agrado que a possibilidade de recurso está prevista através do Supremo Tribunal Federal e, em última análise, da Corte Interamericana de Direitos Humanos.

(109) O CEPD entende que, no contexto das atividades de inteligência nacional, os titulares dos dados dispõem i) dos direitos consagrados na LGPD (em consequência da decisão do Supremo Tribunal Federal de 15 de setembro de 2022), ii) do direito de obter acesso e retificação de dados pessoais através da via de recurso constitucional de *Habeas Data*, bem como iii) do direito a indemnização por danos materiais e morais.

(110) O CEPD congratula-se com a existência desses direitos e com o facto de poderem ser invocados através de mecanismos judiciais e administrativos, em especial a CCAI, bem como com o facto de estas vias de recurso estarem acessíveis a todas as pessoas, independentemente da sua nacionalidade.

4. APLICAÇÃO E ACOMPANHAMENTO DO PROJETO DE DECISÃO

(111) No que diz respeito ao acompanhamento e à revisão do projeto de decisão, o CEPD observa que, de acordo com a jurisprudência do TJUE, «atendendo ao facto de o nível de proteção assegurado por um país terceiro ser suscetível de evoluir, incumbe à Comissão, após a adoção de uma decisão nos termos do [artigo 45.º do RGPD] verificar periodicamente se a constatação relativa ao nível de proteção adequado assegurado pelo país terceiro em causa se continua a justificar de facto e de direito. Tal verificação impõe-se, em qualquer caso, quando haja indícios que suscitem dúvidas a este respeito»[81].

(112) O CEPD observa que a revisão da decisão de adequação terá lugar pelo menos de quatro em quatro anos, em conformidade com o artigo 45.º, n.º 3, do RGPD[82].

(113) O CEPD congratula-se com o facto de o projeto de decisão, no seu considerando 230, prever a participação do CEPD na reunião organizada entre a Comissão e as autoridades brasileiras e dedicada à revisão do funcionamento da decisão de adequação. No que diz respeito à participação concreta do CEPD e dos seus representantes na preparação e no processo das futuras revisões periódicas, o CEPD reitera que qualquer documentação pertinente, incluindo

[81] TJUE, acórdão Schrems I, n.º 76. Ver também o artigo 3.º, n.º 4, do projeto de decisão.
[82] Ver considerando 229 e artigo 3.º, n.º 4, do projeto de decisão.

correspondência, deve ser partilhada por escrito com o CEPD com suficiente antecedência em relação às revisões.

Pelo Comité Europeu para a Proteção de Dados

A Presidente

(Anu Talus)