

PARECER/2025/22

I. Pedido

1. A Direção-Geral de Política Externa do Ministério dos Negócios Estrangeiros solicitou à Comissão Nacional de Proteção de Dados (CNPD) que emitisse Parecer sobre o “Acordo de Cooperação entre a República Portuguesa e a República Federativa do Brasil no Domínio da Investigação e Combate à Criminalidade Organizada Transnacional e ao Terrorismo”.
2. No Pedido é feito constar que se trata de “(...) uma nova versão, finalizada do lado português do projeto de Acordo de Cooperação (...)” em que a “nova redação dos artigos 10.º e 11º foram, de uma forma geral, acomodadas as pretensões expressas por essa Comissão Nacional de Proteção de Dados no seu parecer 2025/18, de 9 de fevereiro, quando se pronunciou sobre a primeira versão do texto.”
3. A CNPD emite parecer no âmbito das suas atribuições, enquanto autoridade nacional de controlo dos tratamentos de dados pessoais, conferidas pelo n.º 1 do artigo 43.º e alíneas a9 e c) do n.º 1 do artigo 44.º da Lei n.º 59/2019, de 8 de agosto, que aprova as regras relativas ao tratamento de dados pessoais para efeitos de prevenção, deteção, investigação ou repressão de infrações penais ou de execução de sanções penais, transpondo a Diretiva (UE) 2016/680 do Parlamento e do Conselho, de 27 de abril de 2016.

II. Análise

4. No Parecer/2025/18, de 9 de fevereiro, a CNPD pronunciou-se sobre a proposta de Acordo entre a República Portuguesa e a República Federativa do Brasil no domínio da investigação e combate à criminalidade organizada transnacional e ao terrorismo, tendo apresentado cinco recomendações:
 - a) “O acordo deve conter normas que supram a falta de legislação de proteção de dados neste domínio, para que estejam asseguradas as garantias adequadas de proteção de dados pessoais previstas pelo Direito português e pelo Direito da União Europeia;
 - b) Devem ser especificadas as finalidades explícitas dos tratamentos de dados pessoais abrangidos pelo Acordo e indicadas as categorias de dados pessoais que lhes estão associadas;
 - c) O Acordo deve conter obrigações relativas à segurança dos tratamentos de dados pessoais, devendo os meios e condições efetivas em que ocorrem as transferências internacionais de dados ser melhor clarificados;

- d) Deve igualmente conter normas para reconhecer e garantir o exercício dos direitos dos titulares dos dados, bem como as condições específicas em que tais direitos podem ser derogados;
- e) O Acordo deve conter normas relativas às vias de recurso administrativas e/ou judiciais para os titulares dos dados, as quais devem ser garantidas em relação a qualquer tratamento de dados pessoais resultante deste Acordo.”

5. No acordo, ora em análise, relativamente à matéria objeto de apreciação, verifica-se que aos artigos 9.º, 10.º e 11.º foi dada nova redação, e que foi aditado um Anexo, com o título: “Definições, tratamento e categorias de dados pessoais”.

6. O artigo 9.º, com a epígrafe “Informação classificada”, que foi introduzido nesta versão, vem remeter a regulação de informação classificada trocada entre as Partes para o Acordo para a Proteção de Informação Classificada entre a República Portuguesa e a República Federativa do Brasil, assinado no Porto em 13 de outubro de 2005, aprovado pelo Decreto n.º 22/2006, de 22 de setembro e em vigor entre as Partes desde 31 de outubro de 2008.”

7. Esse Acordo, aprova estabelece as regras de segurança aplicáveis a todos os acordos de cooperação ou contratos que prevejam a transmissão de informação classificada, celebrados ou a celebrar pelas entidades nacionais competentes das Partes ou por pessoas singulares ou coletivas autorizadas para esse efeito, (artigo 1.º), sendo as entidades nacionais de segurança responsáveis pela aplicação do Acordo: pela República Portuguesa a Autoridade Nacional de Segurança, Presidência de Conselho de Ministros e pela República Federativa do Brasil.

8. Dispõe o artigo 5.º do Acordo que as Partes atribuirão a toda a informação classificada transmitida, produzida ou desenvolvida o mesmo grau de segurança atribuído à sua própria informação classificada de grau equivalente (alínea a)), e que o acesso à informação classificada é limitado às pessoas que tenham necessidade de conhecer e que, no caso de informação classificada como «Confidencial» ou superior, estejam habilitadas com uma credenciação de segurança de pessoa singular emitida pelas autoridades competentes (alínea b). Prevê ainda, o n.º 2 do mesmo artigo que: “Com o objetivo de se obterem e manterem padrões de segurança comparáveis, as entidades nacionais de segurança deverão, sempre que solicitado, disponibilizar mutuamente informação sobre os seus padrões de segurança, procedimentos e práticas para a proteção de informação classificada.”

9. O artigo 9.º estabelece que a informação classificada será transmitida entre as Partes através de canais aprovados conjuntamente pelas entidades nacionais de segurança, (alínea a)) e que as Partes podem transmitir informação classificada por meios eletrónicos, de acordo com os procedimentos de segurança aprovados conjuntamente pelas entidades nacionais de segurança.

10. O artigo 10.º impõe que a informação classificada transmitida só poderá ser utilizada para os fins que foi transmitida e ainda que cada Parte assegurará que todas as pessoas singulares e coletivas que recebam informação classificada respeitem as obrigações do presente Acordo a que acresce a obrigação da Parte destinatária não transmitir informação classificada a uma terceira Parte sem autorização prévia escrita da Parte transmissora.

11. Estas regras foram incorporadas no artigo 10.º e 11.º do Acordo em análise.

12. Neste Acordo prevê-se agora:

- a) no n.º 9 do artigo 11.º, que a verificação do incumprimento do disposto relativamente ao tratamento e transferência de dados pessoais é da responsabilidade de uma autoridade de controlo independente "(...) que seja competente em cada uma das Partes, pelas regras de proteção de dados pessoais.";
- b) na alínea d) do n.º 3 do artigo 11.º que os dados pessoais "utilizados ou transferidos" têm que ser conservados de forma a permitir a identificação das pessoas em causa apenas durante o período necessário para a prossecução das finalidades para que foram recolhidos ou para que são tratados posteriormente, sendo eliminados após esse período; e ainda
- c) no n.º 7 do artigo 11.º que as partes se comprometem a adotar todas as medidas de segurança da informação, nomeadamente contra o acesso indevido ou não autorizado aos dados de natureza pessoal, sendo responsáveis em caso de transmissão incorreta ou não autorizada dos referidos dados.

13. Contudo, "Confidencialidade" e "Informação classificada" não se confundem, nem equivalem a proteção de dados pessoais, pelo que, a invocação do Acordo de 2005 não é suficiente para dar resposta às insuficiências assinaladas no Parecer/2025/18, de 9 de fevereiro, como o não são as regras introduzidas e elencadas em 13.º.

14. Com efeito, as alterações introduzidas, ainda que se saúdem, não foram de molde a densificar as afirmações de princípio que constavam no artigo 10.º da Proposta de Acordo.

15. Como se assinalou no Parecer/2025/18, de 9 de fevereiro, relativamente à segurança do tratamento de dados sujeitos a transferências internacionais é necessário a adoção pelas Partes de medidas técnicas e organizativas adequadas, de acordo com o exigido pelo artigo 31.º da Lei n.º 59/2019.

16. O que neste Acordo se prevê é a confidencialidade da informação classificada, sendo que as garantias dadas pelo artigo 11.º do Acordo para a Proteção da Informação Classificada são inferiores às consagradas no artigo 31.º da Lei n.º 59/2019, de 8 de agosto.

17. Recorda-se ainda que a transferência de dados pessoais para um país terceiro pode ser efetuada com base numa decisão de adequação da Comissão Europeia, como prevê o artigo 38.º, n.º 1 da Lei 59/2019, sendo que o Brasil não goza de uma decisão de adequação.

18. Em consequência, apenas podem ser efetuadas transferências se forem apresentadas pelos responsáveis pelo tratamento garantias adequadas e na condição de os titulares gozarem de direitos oponíveis e terem vias de recurso eficazes disponíveis (alínea a) do n.º 1 do artigo 39º da citada Lei), sendo garantido um nível adequado de proteção equivalente ao assegurado na União Europeia.

19. No Brasil a Lei 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados, garante a privacidade dos dados pessoais, mesmo nos casos em que os dados alvo de tratamento sejam provenientes de fora do território nacional desde que resultem de comunicação ou uso compartilhado de dados com agentes de tratamento brasileiros, desde que o país de proveniência proporcione grau de proteção adequado àquela Lei (artigo 4.º, Inciso IV).

20. Contudo, a Lei 13.709, não é aplicável ao tratamento de dados pessoais realizados para fins exclusivos de segurança pública, defesa e atividades de investigação e repressão de infrações penais, (artigo 4.º, inciso III, al. d)).

21. Alerta-se também para a redação da alínea c) do n.º 3 do artigo 11.º quando estatui que [os dados pessoais] têm que estar corretos e, se necessário, atualizados, devendo ser tomadas todas as medidas razoáveis para assegurar que os dados incompletos (...) sejam eliminados ou retificados, (sublinhado nosso).

22. Ora, um dos princípios que enforma o tratamento dos dados pessoais é precisamente o da exatidão – alínea d) do n.º 2 do artigo 4.º da Lei n.º 59/2019, de 8 de agosto – pelo que, [os dados pessoais] são “Exatos e atualizados sempre que necessário (...)”. Verifica-se que a expressão “necessário” tem no Acordo um sentido diferente do da Lei citada, que importa corrigir. A palavra “necessário” deverá seguir-se à palavra “atualizados” para que o sentido da Lei seja cumprido.

23. O parágrafo 1.º dispõe que “O tratamento de dados pessoais previsto no Inciso III será regido por legislação específica.

24. Tal legislação, contudo, não foi ainda aprovada, existindo ainda um vazio legislativo nesta matéria.

25. Pelo que, o texto do Acordo deverá conter todas as normas que garantam que o nível de proteção dos dados tratados ao abrigo do presente instrumento é essencialmente equivalente ao garantido na União.

26. Deve ainda prever-se a obrigação da Parte requerida notificar a Parte recetora dos dados sempre que estes careçam de retificação, devam ser apagados, ou sujeitos a outras restrições, devendo ser prevista consequentemente a obrigação de a Parte recetora dar cumprimento a esta notificação.

III. Conclusão

27. Nos termos e com os fundamentos expostos, a CNPD recomenda:

- a) O Acordo deve conter normas que supram a falta de legislação de proteção de dados neste domínio na República Federativa do Brasil, para que estejam asseguradas as garantias adequadas de proteção de dados pessoais previstas pelo direito português e da União;
- b) O Acordo deve conter obrigações concretas relativas à segurança dos tratamentos de dados pessoais, devendo os meios e condições efetivas em que ocorrem as transferências internacionais de dados ser melhor clarificados.
- c) A redação da alínea c) do n.º 3 do artigo 11.º deverá ser retificada por forma a que o seu teor corresponda ao da alínea d) do n.º 2 do artigo 4.º da Lei n.º 59/2019, de 8 de agosto, ou seja: [os dados pessoais] são “Exatos e atualizados sempre que necessário (...)”.

Lisboa, 17 de fevereiro de 2025

Paula Meira Lourenço (Presidente)

Assinado por: **PAULA CRISTINA MEIRA LOURENÇO**
Data: 2025.02.17 13:53:33+00'00'
Certificado por: **Diário da República**
Atributos certificados: **Presidente - Comissão Nacional de Proteção de Dados**

