

PARECER/2026/16

I. Pedido

1. Foi submetido à apreciação da Comissão Nacional de Proteção de Dados (CNPD) o projeto de Acordo bilateral entre a República Portuguesa e o Reino de Espanha sobre prevenção e combate à criminalidade organizada transnacional e ao terrorismo (doravante, "Acordo").
2. A presente pronúncia é emitida ao abrigo do disposto no artigo 43.º, n.º 1, e no artigo 44.º, n.º 1, alíneas a) e c), da Lei n.º 59/2019, de 8 de agosto, enquanto autoridade nacional de controlo competente no domínio da proteção de dados pessoais tratados para fins de prevenção, investigação, deteção e repressão de infrações penais.

II. Enquadramento jurídico da cooperação policial transfronteiriça

3. A cooperação policial transfronteiriça no espaço da União Europeia encontra-se amplamente enquadrada por instrumentos jurídicos europeus e internacionais, designadamente:
 - os artigos 40.º e 41.º da Convenção de Aplicação do Acordo de Schengen (vigilância e perseguição transfronteiriça);
 - a Diretiva (UE) 2023/977, relativa ao intercâmbio de informações entre autoridades de aplicação da lei;
 - o Regulamento (UE) 2024/982 (Prüm II), quanto ao intercâmbio automatizado de dados;
 - o Regulamento (UE) 2016/794, no âmbito da cooperação com a Europol;
 - a Diretiva (UE) 2016/680, relativa à proteção de dados no domínio penal, transposta pela Lei n.º 59/2019.
4. Sempre que o Acordo preveja intercâmbio de informações entre autoridades de aplicação da lei dos Estados-membros, tal intercâmbio encontra-se sujeito ao regime harmonizado estabelecido pela Diretiva (UE) 2023/977, que regula os pedidos de informação, os canais de comunicação, os prazos, os fundamentos de recusa e as garantias aplicáveis.
5. Acresce que, sempre que estejam em causa mecanismos de consulta automatizada ou intercâmbio estruturado de dados biométricos (ADN, dados dactiloscópicos, imagens faciais) ou ficheiros policiais, é aplicável o regime diretamente vinculativo estabelecido pelo Regulamento (UE) 2024/982 (Prüm II), o qual define exaustivamente as condições técnicas, procedimentais e de proteção de dados para tais operações. Instrumentos bilaterais não podem instituir mecanismos automatizados paralelos, funcionalmente equivalentes ou menos garantísticos fora desse quadro harmonizado.

6. A celebração de acordos bilaterais neste domínio é admissível, desde que compatível com o quadro jurídico da União, não podendo tais instrumentos reduzir o nível de garantias estabelecido pelo direito europeu nem instituir mecanismos que contornem os regimes estruturados de cooperação policial e judiciária já existentes.
7. Importa salientar que a presente pronúncia se circunscreve à análise das implicações do Acordo no domínio da proteção de dados pessoais, nos termos das competências atribuídas à CNPD pelos artigos 43.º e 44.º da Lei n.º 59/2019, de 8 de agosto. A delimitação entre cooperação policial e cooperação judiciária é apreciada apenas na medida em que projete efeitos sobre o regime jurídico aplicável ao tratamento de dados pessoais.

III. Questões estruturais do Acordo

III.1. Delimitação material: cooperação policial preventiva e processo penal

8. A primeira questão estruturante consiste em determinar se o Acordo se destina exclusivamente à cooperação policial preventiva/operacional ou se admite cooperação concomitante a processo penal instaurado.
9. No ordenamento jurídico português, a investigação criminal em sentido técnico corresponde ao inquérito, dirigido pelo Ministério Público (artigo 219.º da Constituição). Perante notícia de crime, a instauração de inquérito constitui dever funcional do Ministério Público.
10. Sempre que exista processo penal instaurado e estejam em causa atos com valor probatório, diligências intrusivas ou medidas sujeitas a autorização judicial, a cooperação deverá ser enquadrada pelos instrumentos próprios de cooperação judiciária internacional e pelo direito processual aplicável.
11. O Acordo não pode constituir fundamento autónomo para tais atos.
12. O artigo 1.º, n.º 2, ao excluir expressamente o auxílio judiciário mútuo, aponta no sentido de delimitar o âmbito do Acordo à cooperação policial de natureza preventiva e operacional.

III.2. Tensão interna entre artigo 1.º, n.º 2, e artigo 3.º, n.º 1. Técnicas especiais e transmissão de produto concreto.

13. O artigo 1.º, n.º 2, exclui expressamente o auxílio judiciário mútuo.
14. A partilha de informação estratégica sobre técnicas de investigação pode integrar cooperação policial preventiva.
15. Todavia, o artigo 3.º, n.º 1, alíneas c) e d), ao referir “grupos mistos de investigação”, “entregas controladas” e “interceção de comunicações”, aproxima-se, do ponto de vista material, de domínios que:
 - envolvem atos processuais;
 - podem convocar reserva de juiz;

- exigem cadeia de custódia e disciplina probatória.

16. A redação atual permite uma interpretação suscetível de configurar, na prática, mecanismo funcionalmente paralelo à cooperação judiciária, o que deve ser evitado mediante clarificação expressa, de molde que seja inequívoco que o que se pretende é exclusivamente cooperação policial de natureza estratégica, operacional ou metodológica.
17. Deve, assim, resultar claro que o âmbito do artigo 3.º, n.º 1, alínea d), se limita ao intercâmbio de informação de natureza meta-operacional - designadamente boas práticas, metodologias operacionais, experiências comparadas, enquadramento técnico e coordenação estratégica entre autoridades policiais - não abrangendo a prática de atos processuais, a transmissão de produto concreto de medidas sujeitas a autorização judicial, nem a circulação de dados pessoais individualizados ou de elementos probatórios integrados em processo penal instaurado.
18. Trata-se, pois, de informação orientada para aperfeiçoamento técnico-operacional e coordenação institucional, e não de circulação de prova ou de dados concretos relativos a pessoas determinadas.
19. Tal clarificação é particularmente relevante para assegurar a articulação com o artigo 1.º, n.º 2, do próprio Acordo, para preservar a competência das autoridades judiciais e para prevenir riscos de invalidade probatória, violação de segredo de justiça ou desconformidade com os regimes europeus e nacionais de cooperação judiciária internacional.
20. O facto de o processo não se encontrar sujeito a segredo de justiça não altera a natureza processual dos elementos probatórios nele integrados nem os converte automaticamente em informação policial de circulação livre.

III.3. Vigilância transfronteiriça (artigo 4.º, n.º 1, al. ª g), em articulação com o art.º 11.º)

21. A promoção de atividades de vigilância transfronteiriça, prevista no artigo 4.º, n.º 1, alínea g), deve ser lida em articulação com o artigo 11.º do Acordo, que salvaguarda expressamente os direitos e as obrigações decorrentes de outras convenções internacionais de que ambas as Partes sejam partes.
22. Tal implica, na prática, que a referência à vigilância transfronteiriça não constitui criação de um regime autónomo nem ampliação de poderes, devendo ser interpretada como remissão para os quadros jurídicos internacionais já vigentes, designadamente o regime estabelecido nos artigos 40.º e 41.º da Convenção de Aplicação do Acordo de Schengen, permanecendo a sua execução subordinada ao direito interno da Parte em cujo território a atuação ocorre.

IV. Proteção de dados no domínio penal

IV.1. Pessoas suspeitas

23. O Acordo prevê intercâmbio de informação sobre “pessoas suspeitas” sem densificação da categoria.

24. Nos termos do artigo 9.º da Lei n.º 59/2019, deve estabelecer-se, sempre que aplicável e possível, uma distinção clara entre categorias de titulares (suspeitos, condenados, vítimas, testemunhas e terceiros), sem prejuízo da observância dos princípios gerais do tratamento previstos no artigo 4.º do mesmo diploma.
25. Importa ainda salientar que, no plano europeu, a noção de “suspeito” encontra-se densificada pela Diretiva (UE) 2016/680 e é expressamente convocada pelo Regulamento (UE) 2024/982, não podendo assumir extensão autónoma ou indeterminada em instrumentos bilaterais. A utilização dessa categoria no Acordo deve, por conseguinte, ser interpretada de forma conforme ao direito da União, evitando ampliações materiais suscetíveis de comprometer o princípio da presunção de inocência ou de permitir tratamentos excessivos.
26. A transmissão de dados relativos a pessoas suspeitas deve:
- a) assegurar a distinção entre dados baseados em factos e dados baseados em apreciações pessoais ou inferências operacionais, bem como a verificação da exatidão, atualidade e fiabilidade dos dados antes da sua transmissão, em conformidade com o princípio da qualidade dos dados e nos termos do artigo 10.º da Lei n.º 59/2019.
 - b) assegurar que a transmissão identifique expressamente a finalidade prosseguida, em respeito pelo princípio da limitação das finalidades (artigo 4.º, n.º 2, alínea b), da Lei n.º 59/2019), cabendo à autoridade transmissora informar o destinatário das condições aplicáveis ao tratamento (artigo 8.º, n.º 3);
 - c) respeitar o princípio da minimização dos dados, previsto no artigo 4.º, n.º 2, alínea c);
 - d) salvaguardar a presunção de inocência, consagrada no artigo 48.º da Carta dos Direitos Fundamentais da União Europeia.
27. A ausência de densificação normativa quanto à qualificação de “pessoa suspeita” e às condições da sua transmissão pode gerar riscos de tratamento desproporcionado, estigmatização indevida e conservação excessiva ou prolongamento indevido do tratamento.

IV.2. Conservação e revisão periódica

28. A Diretiva (UE) 2016/680, no seu artigo 5.º, e a Lei n.º 59/2019, designadamente nos artigos 4.º, n.º 2, alínea e), e 12.º, impõem que os dados pessoais sejam conservados apenas durante o período necessário às finalidades que justificaram o seu tratamento, devendo ser fixados prazos adequados de apagamento ou de revisão periódica da necessidade da sua manutenção.

29. No âmbito do Regulamento (UE) 2024/982, os dados intercambiados permanecem igualmente sujeitos aos prazos e regras de conservação estabelecidos na Diretiva (UE) 2016/680, não podendo a circulação transfronteiriça conduzir, por força exclusiva da transmissão, a uma extensão automática ou indefinida da sua conservação.
30. Importa igualmente assegurar que qualquer retransmissão subsequente de dados pessoais a outras autoridades, Estados terceiros ou organizações internacionais permaneça sujeita às condições e limitações impostas pela autoridade que procedeu à transmissão inicial, em conformidade com o regime previsto na Diretiva (UE) 2016/680 e na Lei n.º 59/2019.
31. O Acordo não contém disciplina mínima quanto a prazos de conservação, critérios de revisão periódica ou mecanismos de eliminação coordenada entre as Partes. Tal omissão pode gerar assimetrias entre ordenamentos e prolongamentos indevidos do tratamento, designadamente quando a circulação transfronteiriça conduza, na prática, à manutenção de dados cuja necessidade já não subsista no Estado de origem, com risco de violação do princípio da proporcionalidade e do artigo 35.º da Constituição da República Portuguesa.
32. A Comissão Nacional de Proteção de Dados já identificou, em parecer recente relativo a projetos de interoperabilidade no domínio da justiça e da investigação criminal (cf. Parecer n.º 4/2026 da CNPD), insuficiências estruturais associadas à ausência de densificação das categorias de dados transmitidos, à remissão excessiva para regulamentação técnica futura, à indefinição de mecanismos de segurança e rastreabilidade e à falta de disciplina adequada sobre conservação e eliminação.
33. Embora o presente Acordo tenha natureza distinta, apresenta pontos de contacto relevantes com essas preocupações, ao prever interoperabilidade técnica (rádio e geolocalização), intercâmbio de dados relativos a “pessoas suspeitas” e vigilância transfronteiriça, sem densificação suficiente do regime de conservação.
34. A interoperabilidade, quando implique acesso estruturado, automatizado ou sistemático a dados pessoais, pode configurar interconexão funcional de sistemas, exigindo base legal clara e determinada, delimitação de perfis de acesso, bem como mecanismos de registo e auditoria das operações, à luz do artigo 35.º, n.º 4, da Constituição. A experiência nacional demonstra que a mera vedação de acesso ou o arquivamento eletrónico não substituem o apagamento efetivo quando legalmente exigido, podendo a conservação indefinida revelar-se desproporcionada à luz do princípio da necessidade e da jurisprudência europeia em matéria de retenção de dados¹.

¹ Convém citar jurisprudência do Tribunal Europeu dos Direitos Humanos, uma vez que existem direitos fundamentais e necessidade de os mesmos serem respeitados (implementados).

No Acórdão do Tribunal Europeu dos Direitos Humanos de 04/12/2008 (Requerimentos n.ºs 30562/04 e 30566/04; *Marper*), o Tribunal Europeu dos Direitos Humanos considerou que a retenção indefinida das impressões digitais, amostras de células e perfis de ADN era desproporcionada e desnecessária numa sociedade democrática, considerando que o processo penal tinha terminado com uma absolvição:

«125. O Tribunal considera que a natureza geral e indiferenciada do poder de retenção de impressões digitais, amostras biológicas e perfis de DNA de pessoas suspeitas de terem cometido crimes, mas não condenadas, conforme aplicado aos requerentes no presente caso, não reflete um equilíbrio justo entre os interesses públicos e privados concorrentes em jogo, e que o Estado demandado excede

35. Estas preocupações assumem especial relevo no contexto transfronteiriço, onde a ausência de sincronização de prazos ou de mecanismos de eliminação coordenada pode amplificar o risco de conservação prolongada e de diluição de responsabilidades institucionais.
36. Sem exigir que o Acordo reforme os regimes internos das Partes, impõe-se que o seu texto não legitime, ainda que por omissão, prolongamentos indevidos da conservação, não permita interconexões estruturais não densificadas e não remeta integralmente garantias essenciais para futura regulamentação técnica.
37. A interoperabilidade dos sistemas de comunicação rádio deve limitar-se à coordenação operacional quando não envolva tratamento estruturado ou registo sistemático de dados pessoais.
38. Sempre que a interoperabilidade de sistemas de geolocalização implique tratamento de dados pessoais, exige-se base legal clara, delimitação material e temporal, definição de perfis de acesso com registo e auditoria e, quando aplicável, avaliação de impacto sobre a proteção de dados.
39. Qualquer interconexão estrutural que permita cruzamento automatizado de dados deve respeitar o artigo 35.º, n.º 4, da Constituição e os princípios da necessidade e proporcionalidade.

IV.3. Interoperabilidade e interconexão

40. A expressão do art.º 4.º, n.º 1, al.ª a), do Acordo “favorecem a interoperabilidade dos sistemas de comunicação rádio e de geolocalização” deve ser entendida, em primeira linha, como referência à compatibilidade técnica e à coordenação operacional dos meios de comunicação utilizados pelas autoridades policiais das Partes, com vista a permitir a articulação em tempo real de operações transfronteiriças.
41. Tal formulação não deve implicar, por si só, a interconexão estrutural de bases de dados nem o acesso automatizado a sistemas de informação, devendo qualquer tratamento de dados pessoais que daí resulte respeitar o direito interno aplicável e o regime de proteção de dados em vigor.

IV.4. Canais seguros

42. O intercâmbio de informação deve ocorrer através de canais que assegurem confidencialidade, integridade, autenticação forte, rastreabilidade e auditabilidade. O Acordo poderia beneficiar da identificação do canal técnico estruturado a utilizar ou, alternativamente, da exigência de garantias técnicas equivalentes, incluindo registo e auditoria. No plano europeu existem mecanismos estruturados (v.g. Europol/SIENA) e infraestruturas reguladas (v.g.

qualquer margem de apreciação permitida nesta área. Portanto, a retenção impugnada constitui uma interferência desproporcional no direito dos requerentes ao respeito pela sua vida privada e não pode ser considerada necessária numa sociedade democrática...[...].

126. Consequentemente, houve uma violação do artigo 8.º da Convenção no presente caso.»

No Acórdão do Tribunal Europeu dos Direitos Humanos de 06/06/2006 SEGERSTEDT-WIBERG ET AUTRES c. SUÈDE; (Queixa n.º 62332/00), o TEDH constatou uma violação do art.º 8.º da CEDH uma vez que o armazenamento contínuo de dados não era pertinente, devido ao longo período decorrido (cf. ingerência desproporcionada no exercício do direito ao respeito pela vida privada).

Prüm II – Regulamento (UE) 2024/982), devendo o Acordo clarificar se a interoperabilidade prevista se limita à coordenação operacional de meios ou se envolve partilha/consulta de dados pessoais, caso em que se impõem salvaguardas adicionais proporcionais ao risco.

IV.5. Avaliação de risco

43. Atendendo à natureza das operações previstas (vigilância transfronteiriça, dados de localização, interoperabilidade e tratamento de dados relativos a suspeitos), a implementação do Acordo pode configurar um tratamento suscetível de elevado risco.
44. Sempre que o Acordo implique ligação estrutural a bases de dados abrangidas pelo Regulamento (UE) 2024/982, deve ser observada a exigência de avaliação de impacto sobre a proteção de dados prevista na Diretiva (UE) 2016/680 e convocada pelo próprio regime europeu, antes da ligação ou interoperabilidade de sistemas.
45. Nos termos da Lei n.º 59/2019, poderá ser exigível avaliação de impacto (artigo 29.º), registo cronológico das operações (artigo 27.º) e medidas adequadas de segurança (artigo 31.º). Se, após a avaliação, subsistir risco elevado não mitigado, deverá ser equacionada consulta prévia à autoridade de controlo (artigo 30.º).

IV.6. Insuficiência do artigo 8.º (Processamento de dados)

46. O art.º 8.º propõe que «O processamento de dados pessoais entre as Partes, resultante do presente Acordo, é feito em conformidade com o Direito interno das Partes, com a legislação europeia e os compromissos internacionais aplicáveis nesta matéria.»
47. O artigo 8.º do Acordo, tal como apresentado, revela-se insuficiente por se limitar a remissões genéricas, sem consagrar parâmetros operacionais mínimos adequados ao risco das operações previstas.
48. Sem exigir a criação de um regime novo, é recomendável que o Acordo contenha, como já referido, um núcleo mínimo de garantias operacionais de proteção de dados, proporcional ao risco das operações previstas.
49. O Acordo poderia igualmente beneficiar da identificação clara das autoridades responsáveis pelo tratamento de dados pessoais e dos pontos de contacto operacionais entre as Partes, de modo a assegurar a determinação inequívoca das responsabilidades institucionais, a rastreabilidade das transmissões e a efetividade dos mecanismos de supervisão e controlo.

IV.7. Artigo 11.º

50. A cláusula de não-prejuízo constante do artigo 11.º é positiva, sem prejuízo da aplicabilidade direta do direito da União Europeia; poderá, ainda assim, beneficiar de redação que torne mais explícita essa articulação

51. Além disso, tal cláusula não substitui a necessidade de clarificação material das disposições do Acordo suscetíveis de gerar ambiguidades, designadamente no artigo 3.º.

VI. Conclusões

52. A CNPD reconhece a relevância da cooperação policial bilateral no combate à criminalidade organizada transnacional e ao terrorismo e considera que a celebração de instrumentos desta natureza pode constituir um elemento útil de coordenação operacional entre autoridades policiais dos Estados-membros.

53. A presente pronúncia incide exclusivamente sobre a conformidade do Acordo com o quadro jurídico aplicável à proteção de dados pessoais no domínio penal, não se pronunciando sobre a oportunidade política ou diplomática da sua celebração.

54. Para assegurar plena conformidade com o direito da União e com o regime nacional aplicável, revela-se desejável que o Acordo clarifique o seu âmbito material enquanto instrumento de cooperação policial preventiva e operacional, distinguindo-o de mecanismos próprios de cooperação judiciária internacional em matéria penal.

55. Mostra-se igualmente recomendável que o Acordo densifique alguns aspetos essenciais do regime de tratamento de dados pessoais associado à cooperação prevista, designadamente no que respeita:

a) à categoria “pessoas suspeitas”;

b) à explicitação das condições de transmissão de dados pessoais, assegurando a identificação da finalidade do tratamento, a distinção entre dados baseados em factos e dados baseados em apreciações pessoais ou inferências operacionais, bem como a verificação da exatidão, atualidade e fiabilidade dos dados antes da sua transmissão;

c) à previsão de mecanismos adequados de conservação, revisão periódica e eliminação de dados transmitidos no contexto da cooperação transfronteiriça;

d) à clarificação do alcance da interoperabilidade técnica prevista, distinguindo a coordenação operacional entre sistemas de comunicação de eventuais situações de interconexão ou partilha estruturada de dados pessoais;

e) à identificação de canais seguros de comunicação e de requisitos técnicos mínimos que assegurem confidencialidade, integridade, rastreabilidade e auditabilidade das transmissões;

f) à inserção de um núcleo mínimo de garantias operacionais de proteção de dados, proporcional ao risco das operações previstas no art.º 8.º;

g) à clarificação institucional das autoridades competentes em Portugal e Espanha e à articulação com os instrumentos europeus aplicáveis à cooperação policial e ao intercâmbio de informações (v.g. Europol/SIENA).

56. O Acordo apresenta ainda uma tensão entre a exclusão do auxílio judiciário (artigo 1.º, n.º 2) e o conteúdo do artigo 3.º (grupos mistos, entregas controladas, interceções), que deve ser expressamente esclarecida de modo a evitar interpretações suscetíveis de aproximar o Acordo de mecanismos próprios de cooperação judiciária em matéria penal.

57. A CNPD entende que a correção destas insuficiências pode ser alcançada mediante delimitação material clara do âmbito do Acordo, remissões expressas e operativas para os regimes europeus e nacionais aplicáveis e a consagração de um núcleo mínimo de garantias de proteção de dados, designadamente quanto à finalidade, qualidade dos dados, conservação, retransmissão, registo e auditoria das operações, segurança e definição de responsabilidades institucionais.

58. Acresce às insuficiências já identificadas a necessidade de assegurar que o Acordo não seja interpretado ou aplicado de modo a instituir mecanismos de consulta ou intercâmbio automatizado paralelos aos regimes estruturados estabelecidos pelo Regulamento (UE) 2024/982, devendo qualquer interoperabilidade ou partilha estruturada de dados biométricos ou ficheiros policiais respeitar integralmente o quadro harmonizado da União.

Aprovado na reunião de 10 de março de 2026.

Maria Cândida Guedes Oliveira (Vogal em substituição da Presidente)



Assinado por: Maria Cândida
Guedes Machado Antunes de
Oliveira
Identificação: [REDACTED]
Data: 2026-03-11 às 17:23:55