

## PARECER/2026/39

### I. Pedido

1. O Senhor Secretário de Estado da Presidência do Conselho de Ministros solicitou à Comissão Nacional de Proteção de Dados a emissão de Parecer sobre o Projeto de Decreto-Lei (de ora em diante simplesmente designado por Projeto) que altera o Código dos Contratos Públicos, aprovado em anexo ao Decreto-Lei n.º 18/2008, de 29 de janeiro, visando a sua simplificação, clarificação e atualização.
2. O Projeto visa promover a simplificação, digitalização e flexibilização da contratação pública, prevendo, designadamente:
  - a) mecanismos de interoperabilidade administrativa;
  - b) concretização do princípio "só uma vez";
  - c) utilização de sistemas digitais e de inteligência artificial;
  - d) simplificação documental; e
  - e) disponibilização temporária de soluções tecnológicas para fins de avaliação técnica.
3. A CNPD emite parecer no âmbito das suas atribuições e competências enquanto autoridade nacional de controlo dos tratamentos de dados pessoais, conferidas pela alínea c) do n.º 1 do artigo 57.º e pelo n.º 4 do artigo 36.º do Regulamento (UE) 2016/679, de 27 de abril de 2016 – Regulamento Geral sobre a Proteção de Dados (RGPD), em conjugação com o disposto no artigo 3.º, no n.º 2 do artigo 4.º, e na alínea a) do n.º 1 do artigo 6.º, todos da Lei n.º 58/2019, de 8 de agosto.
4. O parecer da CNPD incide exclusivamente sobre as disposições suscetíveis de envolver tratamentos de dados pessoais.

### II. Enquadramento geral

5. No Preâmbulo do Projeto de Decreto-Lei salienta-se as seguintes afirmações:

*«Consagra-se a integração digital da contratação pública, com o reconhecimento da possibilidade de utilização de sistemas digitais, incluindo de inteligência artificial, assim como a identificação dos princípios que devem pautar a utilização destes sistemas, designadamente garantias de interoperabilidade e de proteção de dados.*

*Adicionalmente, simplifica-se e flexibiliza-se a contratação pública, através da desburocratização e consequente redução de custos para os operadores económicos e para as entidades adjudicantes, com a eliminação de documentação declarativa, a concretização do princípio "só uma vez", designadamente ao nível da apresentação de documentos de habilitação.*

*[...] tendo em vista a preparação de procedimentos de formação de contratos públicos que tenham por objeto a aquisição de sistemas e tecnologias de informação, cria-se a possibilidade de as entidades adjudicantes promoverem ou aceitarem a disponibilização gratuita e temporária de soluções tecnológicas para fins de avaliação técnica e de adequação às necessidades públicas subjacentes, com garantias de transparência e de efetiva promoção da concorrência. [...]*»

6. Do Preâmbulo são perceptíveis ideias fundamentais, das quais destacamos como mais relevantes para o presente parecer, a integração digital da contratação pública, incluindo a utilização de sistemas digitais e de inteligência artificial, os mecanismos de interoperabilidade administrativa, a concretização do princípio «só uma vez» e a disponibilização temporária de soluções tecnológicas para fins de avaliação técnica, por constituírem soluções suscetíveis de envolver tratamentos de dados pessoais e de exigir garantias adequadas de proteção de dados.
7. A interoperabilidade administrativa e procedimental não constitui mera realidade técnica ou organizacional, traduzindo igualmente opções juridicamente relevantes quanto à circulação e reutilização de informação pessoal entre entidades públicas.
8. Reitera-se anteriores pronúncias desta Comissão, plasmadas, designadamente nos **Pareceres n.º 13/2015, n.º 38/2015 e n.º 33/2026**, pois verifica-se que propostas normativas assentes em mecanismos de interoperabilidade administrativa, reutilização funcional de informação, plataformas digitais ou soluções algorítmicas tendem recorrentemente a apresentar insuficiente densificação normativa quanto:
  - a) À identificação precisa das categorias de dados pessoais objeto de tratamento, designadamente dados de identificação, dados relativos à idoneidade ou dados constantes de registos administrativos, fiscais ou criminais;
  - b) À definição das responsabilidades pelo tratamento;
  - c) À delimitação dos fluxos de dados;
  - d) À identificação das entidades habilitadas a aceder à informação;
  - e) Às finalidades admissíveis de reutilização;
  - f) Aos mecanismos de rastreabilidade, auditoria e controlo dos acessos;

remetendo frequentemente aspetos materialmente relevantes para regulamentação futura ou soluções técnicas.

9. Neste contexto, torna-se necessário analisar se as soluções previstas no Projeto de Decreto-Lei contêm uma densificação normativa suficiente quanto aos tratamentos de dados pessoais que poderão decorrer da sua aplicação, designadamente em matéria de interoperabilidade administrativa, reutilização de informação, utilização de plataformas digitais e eventual recurso a sistemas de inteligência artificial, bem como

se asseguram garantias adequadas à luz do RGPD, da Lei n.º 58/2019 e do artigo 35.º da Constituição da República Portuguesa (CRP).

### **III. Da necessidade de intervenção legislativa parlamentar**

10. Diversas disposições do Projeto de Decreto-Lei projetam-se diretamente sobre o regime de exercício do direito fundamental à proteção de dados pessoais, designadamente através da previsão de mecanismos de interoperabilidade administrativa, obtenção oficiosa de informação, reutilização documental, agregação informacional, utilização de sistemas digitais e eventual recurso a sistemas de inteligência artificial suscetíveis de envolver tratamentos de dados pessoais.
11. Na medida em que tais soluções podem implicar restrições, condicionamentos ou densificações relevantes do regime de exercício do direito fundamental consagrado no artigo 35.º da Constituição, importa ponderar a respetiva compatibilidade com a reserva relativa de competência legislativa da Assembleia da República prevista no artigo 165.º, n.º 1, alínea b), da CRP.
12. Sem prejuízo da apreciação material das soluções concretamente adotadas, a disciplina dos elementos essenciais dos tratamentos de dados pessoais – designadamente categorias de dados, finalidades, entidades habilitadas ao acesso, condições de reutilização da informação e garantias dos titulares dos dados – deve encontrar suporte normativo adequado à luz das exigências decorrentes daquele preceito constitucional.

### **IV. Da ausência de avaliação de impacto sobre a proteção de dados**

13. O pedido não vem acompanhado por uma Avaliação de Impacto sobre a Proteção de Dados (AIPD), não cumprindo o disposto no n.º 4 do artigo 18.º da Lei n.º 43/2004, de 18 de agosto, na redação introduzida pela Lei n.º 58/2019, de 8 de agosto, segundo o qual os pedidos de parecer relativos a disposições legais e regulamentares em preparação devem ser remetidos à Comissão Nacional de Proteção de Dados instruídos com o respetivo estudo de impacto sobre a proteção de dados.
14. Nos termos do artigo 35.º do RGPD, deve ser realizada uma avaliação de impacto sobre a proteção de dados sempre que um tipo de tratamento, em especial recorrendo a novas tecnologias, seja suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares.
15. Invoca-se aqui o artigo 35.º do RGPD como parâmetro substantivo e não como base direta de obrigatoriedade procedimental.

## V. Considerações gerais

16. A arquitetura normativa projetada assenta em mecanismos de interoperabilidade administrativa, reutilização funcional de informação, plataformas digitais e sistemas potencialmente assistidos por inteligência artificial, envolvendo circulação estruturada de dados entre entidades públicas.
17. Tais mecanismos constituem tratamentos de dados pessoais juridicamente relevantes na aceção do artigo 4.º, n.º 2, do RGPD, podendo suscitar riscos acrescidos de reutilização funcional da informação, agregação de dados provenientes de diferentes contextos administrativos, opacidade dos fluxos informacionais e utilização de mecanismos automatizados de avaliação, categorização, priorização ou apoio à decisão.
18. A dispersão destas soluções ao longo de múltiplas disposições do Código dos Contratos Públicos dificulta a perceção unitária dos tratamentos de dados pessoais, dos fluxos informacionais envolvidos, das responsabilidades pelo tratamento e das garantias aplicáveis. Embora determinados aspetos possam ser objeto de concretização regulamentar ou técnica, a CNPD considera indispensável que o regime densifique os limites da interoperabilidade, as finalidades admissíveis de reutilização, as responsabilidades pelo tratamento, os mecanismos fundamentais de supervisão humana e as garantias mínimas de auditabilidade e rastreabilidade.

## VI. Análise na especialidade

### VI.1. Aquisição de soluções tecnológicas e dependência tecnológica (artigo 24.º, n.º 11)

19. O artigo 24.º, n.º 11 do Projeto admite expressamente o recurso ao ajuste direto na aquisição de bens e serviços no domínio dos sistemas e tecnologias de informação (cf. «*As entidades adjudicantes podem recorrer ao procedimento de ajuste direto, nos termos da alínea c) do n.º 1 e desde que verificados os respetivos pressupostos, designadamente, na aquisição de bens e na prestação de serviços no domínio dos sistemas e tecnologias de informação.*»).
20. A contratação urgente ou simplificada de soluções tecnológicas pode, todavia, criar riscos acrescidos de:
- a) Dependência tecnológica ("lock-in");
  - b) Utilização de sistemas opacos ("*black box*"), isto é, sistemas cuja lógica de funcionamento não é suscetível de explicação ou controlo quanto aos critérios utilizados;
  - c) Insuficiente auditabilidade;
  - d) Reutilização indevida de informação; ou
  - e) Adoção de soluções tecnológicas sem garantias adequadas de proteção de dados.

21. A crescente utilização de plataformas digitais, serviços *cloud*, soluções de inteligência artificial e sistemas automatizados na contratação pública exige que as entidades adjudicantes mantenham controlo efetivo sobre os tratamentos de dados pessoais e sobre os critérios materialmente relevantes suscetíveis de influenciar operações procedimentais ou decisórias, assegurando-se transparência procedimental, supervisão humana significativa e responsabilidade administrativa pelas decisões adotadas.
22. A CNPD considera particularmente importante assegurar que a aquisição e utilização destas soluções observem requisitos adequados de segurança, auditabilidade, explicabilidade, rastreabilidade e proteção de dados desde a conceção e por defeito.
23. Importa igualmente assegurar:
  - a) A clara definição das responsabilidades pelo tratamento e dos deveres dos fornecedores tecnológicos;
  - b) Mecanismos efetivos de supervisão humana significativa, documentação técnica adequada e controlo dos critérios materialmente relevantes utilizados pelos sistemas digitais ou algorítmicos.

## **VI.2. Plataformas eletrónicas, tramitação digital e responsabilidade pelo tratamento (artigos 62.º e 62.º-A)**

24. Os artigos 62.º e 62.º-A do Projeto aprofundam a lógica de:
  - a) Desmaterialização procedimental;
  - b) Tramitação eletrónica;
  - c) Utilização de plataformas digitais;
  - d) Interoperabilidade; e
  - e) Circulação eletrónica de informação.
25. Em especial:
  - a) O artigo 62.º prevê a apresentação eletrónica das propostas através de plataformas eletrónicas; e
  - b) O artigo 62.º-A admite a utilização de catálogos eletrónicos e mecanismos de interligação entre sistemas.
26. A interoperabilidade administrativa e os mecanismos de reutilização documental previstos no projeto pressupõem circulação estruturada de informação entre entidades e plataformas digitais, impondo especial densificação normativa quanto à definição dos fluxos de dados, finalidades de tratamento, critérios de acesso e mecanismos de rastreabilidade.
27. A ausência de definição suficientemente precisa destes elementos dificulta a delimitação funcional dos tratamentos, a verificação da proporcionalidade dos acessos e a efetiva responsabilização pelas operações realizadas em ambiente interoperável.

28. Impõe-se, por isso, assegurar mecanismos efetivos de segregação funcional, rastreabilidade e controlo dos acessos, em conformidade com os princípios da limitação das finalidades, minimização dos dados (cf. art.º 5.º, n.º 1, alíneas b) e c), do RGPD) e proteção de dados desde a conceção e por defeito (cf. artigo 25.º do RGPD).
29. Em matéria de plataformas/catálogos, o Projeto carece de requisitos de segurança, autenticação forte (eIDAS), gestão de perfis/permissoes, logs, retenção, interoperabilidade conforme ENS/EUPL ou normas equivalentes; e proibição de *tracking* além do necessário.

### **VI.3. Interoperabilidade administrativa, reutilização documental e princípio “só uma vez” (artigos 81.º e 83.º-A)**

30. As alterações introduzidas nos artigos 81.º e 83.º-A do Projeto concretizam uma lógica de:
- Interoperabilidade administrativa;
  - Obtenção oficiosa de documentação;
  - Reutilização documental;
  - Agregação informacional; e
  - Simplificação administrativa.
31. Em especial:
- O artigo 81.º, n.º 10, prevê a obtenção oficiosa de informações e documentos através de sistemas de interoperabilidade com outras autoridades públicas; e
  - O artigo 83.º-A admite expressamente soluções de agregação e consulta centralizada de documentos, incluindo carteiras digitais.
32. A concretização do princípio “só uma vez” (“*once only*”), evitando a apresentação repetida de documentação já detida pela Administração Pública, pode revelar-se compatível com os princípios da minimização e da simplificação administrativa.
33. Todavia, a concretização do princípio “só uma vez” pressupõe a circulação estruturada de informação, a interoperabilidade entre sistemas, a reutilização funcional de dados, a consulta automatizada e a eventual agregação informacional.
34. O Projeto de Decreto-Lei não densifica suficientemente os limites funcionais da interoperabilidade administrativa, os critérios de reutilização documental nem os mecanismos de controlo dos acessos realizados em ambiente interoperável.
35. Tal solução suscita reservas à luz do princípio da limitação das finalidades previsto no artigo 5.º, n.º 1, alínea b), do RGPD, do princípio da minimização (artigo 5.º, n.º 1, alínea c), do RGPD) e do artigo 35.º da

CRP e das exigências de densificação normativa inerentes à interconexão e circulação de dados pessoais entre entidades públicas.

### ***VI.3.1. Interoperabilidade e acesso a dados***

36. O Projeto prevê o uso de:

- mecanismos de interoperabilidade para obtenção oficiosa de dados;
- agregação e consulta centralizada de informação em plataformas digitais.

37. À semelhança do já assinalado pela CNPD nos **Pareceres 13/2015 e 33/2026**, que se reiteram, situações de interconexão e interoperabilidade administrativa de dados exigem base legal suficientemente densificada, definição clara dos fluxos de dados, identificação dos responsáveis pelo tratamento, explicitação das categorias de dados e finalidades, limitação funcional dos acessos e mecanismos de rastreabilidade e registo de acessos.

38. Acresce que a obtenção oficiosa de documentação reduz encargos administrativos, mas pode simultaneamente aumentar:

- a) A opacidade dos fluxos informacionais, designadamente quanto às entidades que acedem aos dados, às categorias de dados efetivamente consultadas e às finalidades subjacentes aos acessos realizados;
- b) A invisibilidade dos tratamentos; e
- c) A assimetria informacional relativamente aos titulares dos dados.

### ***VI.3.2. Mecanismos técnicos de vinculação funcional do acesso (“purpose binding técnico”)***

39. O respeito pelo princípio da limitação das finalidades não pode assentar apenas em proibições abstratas de reutilização jurídica dos dados.

40. Impõe-se igualmente a existência de mecanismos técnicos de vinculação funcional do acesso (“*purpose binding* técnico”), assegurando que os dados só podem ser consultados em função de finalidades previamente determinadas:

- a) Segmentação lógica da informação;
- b) Perfis diferenciados de acesso;
- c) Granularidade;
- d) Controlo por finalidade;
- e) *Logs*; e
- f) Rastreabilidade integral dos acessos.

### ***VI.3.3. Garantias mínimas aplicáveis aos mecanismos de interoperabilidade***

41. A CNPD considera, por isso, indispensável que os mecanismos de interoperabilidade administrativa e reutilização documental previstos nos artigos 81.º, n.º 10, e 83.º-A do CCP sejam acompanhados de adequada densificação normativa, quanto à definição dos fluxos de dados, finalidades de reutilização, critérios de acesso, mecanismos de controlo e responsabilidades pelo tratamento.
42. Em particular, tais mecanismos devem assegurar que os acessos a dados pessoais:
- a) Apenas ocorrem para finalidades diretamente relacionadas com o procedimento em causa;
  - b) Se encontram limitados a categorias de dados previamente definidas; e
  - c) São integralmente registados, com indicação da respetiva finalidade.

### **VI.4. Flexibilização procedimental, sistemas digitais e risco de opacidade decisória (artigos 127.º-A e 127.º-B)**

43. Os artigos 127.º-A e 127.º-B do Projeto introduzem o regime de *consulta prévia especial*, reforçando a flexibilidade procedimental em determinados domínios, incluindo:
- a) Transformação digital;
  - b) Aquisição de soluções tecnológicas;
  - c) Serviços *cloud*;
  - d) *Software*; e
  - e) Sistemas informáticos.
44. Embora tais normas não incidam diretamente sobre proteção de dados pessoais, a crescente utilização de plataformas digitais, sistemas automatizados, filtros algorítmicos, mecanismos automatizados de categorização, priorização ou avaliação pode gerar riscos acrescidos de:
- a) Opacidade decisória;
  - b) Discriminação indireta;
  - c) Enviesamento algorítmico, entendido como a produção de resultados sistematicamente desfavoráveis ou discriminatórios decorrentes da estrutura ou dos dados utilizados pelos sistemas automatizados; e
  - d) Insuficiente auditabilidade.
45. A flexibilização procedimental e o reforço da discricionariedade administrativa exigem, por isso, mecanismos acrescidos de transparência, auditabilidade e supervisão humana significativa.

46. Impõe-se o reforço das obrigações de transparência e registos quando usados mecanismos automatizados de triagem/avaliação sob limiares mais altos.
47. Impõe-se igualmente assegurar mecanismos adequados de gestão de riscos, governação dos dados, supervisão humana significativa, registo e rastreabilidade das operações e transparência algorítmica, os quais constituem elementos essenciais para uma utilização conforme de sistemas digitais e de inteligência artificial pela Administração Pública.

**VI.5. Princípios e utilização de sistemas digitais e Inteligência artificial na contratação pública (cf. a utilização de sistemas digitais e de inteligência artificial na contratação pública encontra-se projetada transversalmente em diversas disposições do CCP, assumindo particular relevância os artigos 1.º-C, 24.º, n.º 11, 62.º, 62.º-A, 81.º, n.º 10, 83.º-A, 127.º-A e 127.º-B)**

48. O Projeto reconhece a possibilidade de utilização de sistemas digitais, incluindo sistemas de inteligência artificial, na contratação pública.
49. O artigo 1.º-C (Contratação pública digital) do Projeto já elenca princípios, faltando, todavia, operacionalização mínima quanto à definição de supervisão humana, documentação, auditabilidade, registo das operações e mecanismos de contestação.
50. A consagração da utilização de sistemas digitais e de inteligência artificial na contratação pública deve ser articulada com:
  - a) Os princípios gerais da atividade administrativa;
  - b) O novo enquadramento principiológico do diploma;
  - c) O RGPD;
  - d) O Regulamento da Inteligência Artificial; e
  - e) Os princípios da transparência, explicabilidade, não discriminação e controlo humano significativo.
51. Sem prejuízo da concreta qualificação jurídica dos sistemas eventualmente utilizados, e convocando o Regulamento (UE) 2024/1689, de 13 de junho de 2024 (Regulamento da Inteligência Artificial), como referencial normativo relevante, assumem especial importância os requisitos relativos à gestão de riscos, governação e qualidade dos dados, transparência, supervisão humana, exatidão, robustez, cibersegurança e rastreabilidade dos sistemas utilizados pela Administração Pública.
52. Em particular, assumem especial relevância, como referenciais prudenciais de conformidade, os requisitos aplicáveis aos sistemas de Inteligência Artificial (IA) de risco elevado (artigos 6.º e 8.º), os deveres de gestão de riscos (artigo 9.º), as exigências de governação e qualidade dos dados (artigo 10.º), os deveres de

transparência (artigo 13.º), os mecanismos de supervisão humana (artigo 14.º), os requisitos de exatidão, robustez e cibersegurança (artigo 15.º), bem como as obrigações das entidades responsáveis pela utilização de sistemas de inteligência artificial previstas no artigo 26.º do Regulamento da Inteligência Artificial (UE) 2024/1689.

53. Todavia, o diploma não densifica as finalidades admissíveis, as operações concretamente automatizadas, os limites funcionais da utilização de IA, os mecanismos de supervisão humana, os deveres de auditabilidade e os mecanismos de explicabilidade.
54. A utilização de sistemas algorítmicos em procedimentos de contratação pública pode envolver:
- a) Avaliação automatizada;
  - b) Categorização de operadores económicos;
  - c) Mecanismos automatizados de categorização, priorização ou avaliação;
  - d) Análise preditiva;
  - e) Detecção de risco ou idoneidade;
  - f) Priorização procedimental; ou
  - g) Análise automatizada documental de operadores económicos e propostas.
55. Tais operações podem aproximar-se de mecanismos automatizados de avaliação, categorização ou priorização e podem suscitar questões à luz do artigo 22.º do RGPD, exigindo especial conformidade com os princípios da transparência e responsabilidade e as exigências de supervisão humana significativa.

#### ***VI.5.1. Mecanismos automatizados de categorização, priorização ou avaliação, AI Act e transparência algorítmica***

56. A previsão de utilização de sistemas digitais e, potencialmente, de inteligência artificial no âmbito da contratação pública exige apreciação à luz dos recentes desenvolvimentos jurisprudenciais e normativos europeus.
57. Desde logo, o Tribunal de Justiça da União Europeia afirmou, no **Acórdão SCHUFA, de 7 de dezembro de 2023 (C-634/21, EU:C:2023:957)**, que a determinação automatizada de um valor de probabilidade (“score”), quando utilizada de forma determinante para decisões relativas ao estabelecimento, execução ou cessação de relações jurídicas, pode já constituir uma decisão automatizada na aceção do artigo 22.º do RGPD.
58. Embora o referido Acórdão respeitasse ao setor financeiro, a respetiva fundamentação revela-se particularmente relevante no domínio da contratação pública digital, na medida em que sistemas algorítmicos podem influenciar materialmente:
- a) A avaliação de propostas;
  - b) A apreciação da capacidade técnica ou económica;

- c) A deteção de risco;
  - d) A priorização procedimental; ou
  - e) Outras decisões suscetíveis de afetar significativamente operadores económicos.
59. No domínio da contratação pública, a transparência algorítmica assume particular relevância, na medida em que assegura a igualdade de tratamento, previne discriminações indiretas, favorece a auditabilidade e permite o controlo jurisdicional das decisões administrativas.
60. A CNPD já assinalou igualmente, no **Parecer n.º 33/2026**, que a crescente utilização de mecanismos algorítmicos e sistemas digitais na Administração Pública exige especial atenção no que concerne à:
- a) Inteligibilidade dos critérios decisórios;
  - b) Transparência procedimental;
  - c) Auditabilidade;
  - d) Supervisão humana significativa; e
  - e) Preservação do controlo jurisdicional efetivo.
61. O respeito pelo princípio da transparência não pode limitar-se à mera informação abstrata sobre a existência de sistemas automatizados, exigindo igualmente a possibilidade de controlo material da lógica subjacente às decisões produzidas ou significativamente influenciadas por tais sistemas.
62. A CNPD considera, por isso, indispensável que o regime jurídico assegure:
- a) Avaliação de conformidade;
  - b) Qualidade dos dados utilizados;
  - c) Explicabilidade adequada dos modelos;
  - d) Rastreabilidade das operações algorítmicas;
  - e) Auditorias independentes;
  - f) Mecanismos de contestação; e
  - g) Supervisão humana significativa.
63. A utilização de sistemas algorítmicos no contexto da contratação pública deverá, por conseguinte, observar cumulativamente:
- a) O artigo 22.º do RGPD;
  - b) Os princípios da licitude, necessidade e minimização;
  - c) As exigências de proteção de dados desde a conceção e por defeito; e
  - d) O quadro regulatório europeu aplicável à inteligência artificial.
64. A utilização de sistemas de inteligência artificial que influenciem operações procedimentais ou decisórias deve assegurar:
- a) Documentação técnica adequada;

- b) Possibilidade de explicação dos critérios utilizados;
- c) Supervisão humana significativa;
- d) Mecanismos de revisão e contestação das decisões.

#### **VI.6. Soluções tecnológicas gratuitas (artigo 35.º-C)**

90. O Projeto de diploma prevê a possibilidade de disponibilização gratuita e temporária de soluções tecnológicas para fins de avaliação técnica e adequação às necessidades públicas.
91. Deve, desde logo, assinalar-se positivamente a previsão de requisitos em matéria de publicidade, proteção de dados, reversibilidade e proibição de contrapartidas ocultas.
92. Não obstante, o regime suscita preocupações relevantes em matéria de proteção de dados pessoais, na medida em que pode permitir o acesso por operadores económicos a fluxos informacionais associados à contratação pública, bem como a reutilização, agregação ou utilização de dados para desenvolvimento ou aperfeiçoamento de sistemas automatizados, podendo ainda gerar situações de dependência tecnológica.
93. O regime não densifica suficientemente as garantias aplicáveis, designadamente quanto às condições de acesso aos dados, à segregação dos ambientes de teste, à anonimização ou pseudonimização, ao apagamento dos dados ou à existência de mecanismos de auditoria.
94. Embora o artigo 35.º-C, n.º 3, consagre a proibição de reutilização de dados para fins próprios dos operadores económicos, incluindo treino, validação ou melhoria de modelos, subsistem insuficiências quanto à densificação dos limites e condições de acesso aos dados no contexto da avaliação técnica, designadamente no que respeita à:
- a) Delimitação do que seja «estritamente necessário» à execução do teste;
  - b) Prevenção de utilizações indiretas ou derivadas dos dados; e
  - c) Articulação com o princípio da limitação das finalidades consagrado no RGPD.
95. Em particular, a disponibilização destas soluções deve assegurar que:
- a) Não ocorre qualquer reutilização de dados para finalidades próprias dos operadores económicos;
  - e
  - b) O acesso a dados pessoais se encontra estritamente limitado ao necessário para a execução do teste, devendo ser assegurada, sempre que possível, a segregação dos ambientes de teste e a anonimização dos dados.

#### VI.7. Critérios de adjudicação e avaliação automatizada (artigos 74.º e 75.º do Projeto de Decreto-Lei)

96. A eventual utilização de modelos automatizados ou assistidos por IA na avaliação de propostas suscita questões de:
- Mecanismos automatizados de avaliação ou categorização;
  - Decisões automatizadas;
  - Transparência dos critérios.
97. Nos termos do artigo 22.º do RGPD, deve ser assegurado que não há decisões exclusivamente automatizadas com efeitos significativos e que existe intervenção humana adequada.
98. Afigura-se-nos necessária a previsão de auditabilidade dos modelos, possibilidade de explicação dos resultados e direito dos concorrentes a contestação.

#### VI.8. Direitos dos titulares e transparência

99. À semelhança do identificado no **Parecer n.º 38/2015 desta CNPD**, permanece insuficientemente densificada:
- A garantia dos direitos de informação, acesso e transparência relativamente aos tratamentos de dados pessoais realizados em ambiente interoperável e digital, nos termos dos artigos 12.º a 15.º do RGPD;
  - A definição dos critérios e prazos de conservação dos dados pessoais tratados no âmbito das plataformas, mecanismos interoperáveis e sistemas digitais previstos no regime projetado, à luz do princípio da limitação da conservação consagrado no artigo 5.º, n.º 1, alínea e), e do artigo 25.º do RGPD;
  - A identificação clara das entidades responsáveis pelo tratamento e das respetivas responsabilidades, designadamente em contextos de interoperabilidade administrativa, utilização de plataformas digitais e recurso a fornecedores tecnológicos, nos termos dos artigos 4.º, n.º 7, 24.º, 26.º e 28.º do RGPD.
100. Afigura-se igualmente necessária a inclusão de norma autónoma relativa à proteção de dados pessoais aplicável aos procedimentos de formação e execução de contratos públicos, densificando:
- Os limites da interoperabilidade administrativa;
  - Os deveres aplicáveis à utilização de sistemas digitais ou algorítmicos; e
  - Os mecanismos de exercício dos direitos dos titulares.

101. A utilização de sistemas digitais, incluindo sistemas de inteligência artificial, deve ainda assegurar mecanismos de supervisão humana significativa, auditabilidade, rastreabilidade e explicabilidade dos resultados produzidos.
102. Nesse contexto, deverá ser expressamente estabelecido que as entidades adjudicantes atuam como responsáveis pelo tratamento, garantindo a efetividade dos mecanismos de exercício dos direitos dos titulares e a definição clara das responsabilidades aplicáveis aos fornecedores tecnológicos e subcontratantes.
103. Adicionalmente, o Projeto de Decreto-Lei deverá prever expressamente a:
- a) Delimitação das categorias de dados pessoais suscetíveis de tratamento em contexto de interoperabilidade;
  - b) Definição dos fluxos de circulação da informação e das respetivas finalidades;
  - c) Definição das responsabilidades pelo tratamento;
  - d) Consagração de mecanismos obrigatórios de rastreabilidade, incluindo a conservação de registos de acesso (*logs*);
  - e) Adoção de mecanismos de segregação funcional e de controlo de acessos por perfis;
  - f) Garantia de que não ocorre reutilização dos dados para fins próprios dos operadores económicos, designadamente para treino, validação ou melhoria de modelos, nem para quaisquer finalidades incompatíveis com aquelas que presidiram à respetiva recolha;
  - g) Garantia de supervisão humana significativa nos tratamentos automatizados;
  - h) Proibição de decisões exclusivamente automatizadas com efeitos jurídicos ou significativamente relevantes;
  - i) Previsão de deveres de auditabilidade dos sistemas digitais e algorítmicos utilizados;
  - j) Consagração de mecanismos de explicabilidade, revisão e contestação das decisões;
  - k) Definição de regras específicas de conservação e apagamento dos dados; e
  - l) Sujeição dos sistemas interoperáveis, plataformas digitais e soluções tecnológicas a avaliação de impacto sobre a proteção de dados, sempre que possam implicar elevado risco para os direitos e liberdades dos titulares.

## VII. Conclusões

104. Sem prejuízo da margem de conformação do legislador e da admissibilidade de concretização regulamentar e técnica de determinados aspetos operacionais, a CNPD considera que a conformidade do regime

projetado com o artigo 35.º da CRP, com o RGPD e com o Regulamento da Inteligência Artificial, pressupõe a adoção de medidas mínimas de densificação normativa, organizacional e técnica, designadamente:

- a) **A introdução de disposição autónoma relativa à proteção de dados pessoais e utilização de sistemas digitais e algorítmicos, assegurando:** delimitação funcional da interoperabilidade; definição das finalidades admissíveis; identificação dos responsáveis pelo tratamento; garantias de supervisão humana significativa; e mecanismos mínimos de auditabilidade e rastreabilidade;
- b) **A revisão e densificação das disposições respeitantes:** ao artigo 1.º-C; aos artigos 62.º e 62.º-A; aos artigos 81.º e 83.º-A; e ao artigo 35.º-C do CCP;
- c) **A realização de Avaliação de Impacto sobre a Proteção de Dados (AIPD)** relativamente aos mecanismos de interoperabilidade, reutilização documental, plataformas digitais e eventual utilização de sistemas algorítmicos, incluindo mapeamento dos tratamentos, fluxos informacionais, avaliação de necessidade e proporcionalidade, análise de riscos, medidas de mitigação e mecanismos de auditoria e supervisão;
- d) **A definição de modelo de governação compatível com o Regulamento da Inteligência Artificial,** designadamente quanto à gestão de riscos, à governação de dados, à documentação técnica, aos mecanismos de supervisão humana, à rastreabilidade, à robustez e cibersegurança e à avaliação de conformidade;
- e) **A previsão de requisitos mínimos aplicáveis às plataformas eletrónicas e fornecedores tecnológicos,** designadamente em matéria de controlo de acessos, segregação funcional, autenticação forte, gestão de *logs*, retenção, segurança da informação, gestão de incidentes e exercício dos direitos dos titulares;
- f) **A previsão de cláusulas mínimas aplicáveis à contratação de fornecedores tecnológicos e sistemas algorítmicos,** incluindo deveres de documentação, auditabilidade, explicabilidade, testes de enviesamento, limitações à reutilização dos dados e limitação da utilização dos dados para treino algorítmico aos casos em que tal seja juridicamente admissível e compatível com a finalidade da recolha;
- g) **A consagração de mecanismos de explicabilidade, contestação e supervisão humana relativamente a operações procedimentais suscetíveis de serem influenciadas por sistemas automatizados.**
- h) **A adoção de medidas de formação e capacitação dos intervenientes procedimentais** relativamente à utilização responsável de plataformas digitais, à proteção de dados e aos riscos associados à utilização de sistemas automatizados e de inteligência artificial;

- i) **A ponderação da adequação do instrumento legislativo utilizado**, na medida em que diversas disposições do regime projetado disciplinam elementos essenciais de tratamentos de dados pessoais, logo, enquadráveis na reserva relativa de competência legislativa da Assembleia da República prevista no artigo 165.º, n.º 1, alínea b), da Constituição da República Portuguesa.

Aprovado na reunião de 2 de junho de 2026

Paula Meira Lourenço (Presidente)

Assinado por: **PAULA CRISTINA MEIRA LOURENÇO**

Data: 2026.06.02 21:22:32+01'00'

Certificado por: **Diário da República**

Atributos certificados: **Presidente - Comissão Nacional de Proteção de Dados**

