CNPD
Comissão Nacional de Proteção de Dados

PARECER/2026/33

I. Pedido

1. O Senhor Secretário de Estado da Presidência do Conselho de Ministros solicitou à Comissão Nacional de Proteção de Dados (CNPD) a emissão de Parecer sobre o Projeto de Decreto-Lei que estabelece o regime geral de interoperabilidade documental e de dados para a Administração Pública – MARE (Reg. DL 149/XXV/2026).

2. O pedido vem acompanhado por uma Avaliação de Impacto sobre a Proteção de Dados (AIPD), tendo em vista o cumprimento do disposto no n.º 4 do artigo 18.º da Lei n.º 43/2004, de 18 de agosto, na redação dada pela Lei n.º 58/2019, de 8 de agosto, que obriga a que *"os pedidos de parecer sobre disposições legais e regulamentares em preparação devem ser remetidos à CNPD pelo titular do órgão com poder legiferante ou regulamentar, instruídos com o respetivo estudo de impacto sobre a proteção de dados"*, pese embora não corresponda, sob o ponto de vista material, a uma AIPD ao abrigo do disposto no artigo 35.º do Regulamento (UE) 2016/679, de 27 de abril de 2016 (Regulamento Geral sobre a Proteção de Dados), nem siga as orientações da minuta de AIPD do Comité Europeu para a Proteção de Dados (aprovada a 10 de março de 2026 e em consulta pública)[1].

3. A CNPD emite parecer no âmbito das suas atribuições e competências, enquanto autoridade administrativa independente com poderes de autoridade para o controlo dos tratamentos de dados pessoais, conferidos pela alínea *c)* do n.º 1 do artigo 57.º, a alínea *b)* do n.º 3 do artigo 58.º e n.º 4 do artigo 36.º, todos 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, que executa na ordem jurídica interna o RGPD.

4. Nos termos do preâmbulo pretende-se concretizar e operacionalizar o princípio "*once only*", princípio segundo o qual os cidadãos devem apresentar a sua informação apenas uma vez junto da administração pública, não devendo esta solicitar ao cidadão dados de que já dispõe, pelo que se pretende facilitar a transmissão de informação entre entidades da Administração Pública quando essa informação seja produzida pela própria Administração, automatizando a transmissão de documentação e dados entre entidades.

[1] A minuta de AIPD encontra-se disponível no sítio oficial do CEPD na Internet, em: https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2026/edpb-dpia-template_en, por estar em consulta pública até ao dia 9 de junho de 2026.

5. Tendo em conta que a larga maioria da informação transmitida entre entidades configura dados pessoais consagra-se como fundamento de licitude para o seu tratamento a obrigação legal das entidades públicas recorrerem à referida plataforma para a obtenção de toda a documentação gerada ou conservada pela administração publica.

6. Em matéria de âmbito objetivo, fica coberta pelo diploma a prestação de serviços públicos que seja iniciada por iniciativa particular; que seja solicitada por uma entidade administrativa, no âmbito de um procedimento administrativo de iniciativa particular; ou que seja iniciada por uma entidade administrativa, nos termos da lei. Adicionalmente, e desde que o cidadão tenha tomado conhecimento, a interoperabilidade como aqui prevista pode estender-se a serviços conexos do primeiro, isto é, serviços que decorram opcionalmente do primeiro serviço prestado.

II. Análise

a) Forma do Diploma

7. Importa, antes de mais, manifestar preocupação quanto à forma do projeto de diploma em análise, porquanto incidindo o seu regime sobre direitos, liberdades e garantias fundamentais, em particular, sobre o direito fundamental à proteção de dados pessoais, previsto no artigo 35.º da Constituição da República Portuguesa (CRP), e princípios e direitos, liberdades e garantias fundamentais conexos[2], a sua definição é da competência reservada da Assembleia da República, através de Lei (contendo todo o regime legal, e que lhe poderá ser submetida pelo Governo através de uma Proposta de Lei), ou através de Lei de Autorização legislativa concedida ao Governo (que para tanto deverá submeter uma Proposta de Lei de autorização)– cf. alínea *b)* do n.º 1 do artigo 165.º da Constituição da República Portuguesa (CRP). Assim sendo, a CNPD recomenda (em particular quando o projeto de Decreto-Lei em causa pretende alterar uma Lei da Assembleia da República – cf. infra, ponto 24 do presente Parecer) que se reveja a opção legislativa por forma a assegurar que o regime jurídico seja definido em instrumento jurídico idóneo a cumprir a finalidade visada.

[2] Como seja o princípio da igualdade e da não discriminação, em razão de ascendência, sexo, raça, etnia, língua, território de origem, religião, convicções políticas ou ideológicas, instrução, situação económica, condição social ou orientação sexual (artigo 13.º da CRP), do direito à reserva da intimidade da vida privada, à identidade pessoal, à identidade genética do ser humano, ao desenvolvimento da personalidade, ao bom nome, à reputação e à imagem (artigo 26.º da CRP), e bem assim do direito à liberdade (artigo 27.º da CRP) e o direito à liberdade de expressão (artigo 37.º da CRP).

CNPD
Comissão Nacional
de Proteção de Dados

b) Impacto do diploma no direito à proteção de dados pessoais

8. A CNPD tem vindo a alertar em diversos Pareceres emitidos[3] sobre os riscos que a generalização de interconexões, acessos recíprocos e transmissão da informação constante de bases de dados da Administração Pública acarreta para os cidadãos. Com efeito, ainda que se compreenda o objetivo de gestão eficiente da informação e de agilização dos procedimentos administrativos, e a utilidade, para esse efeito, da partilha de informação sobre os cidadãos detida pelo Estado e por outras pessoas coletivas públicas, não podem ser ignorados os riscos daqui decorrentes para os direitos dos cidadãos, sobretudo quando a lei se limita a prever a sua realização sem fixar as garantias adequadas à proteção dos direitos fundamentais das pessoas a quem tais dados dizem respeito e, até mesmo, sem definir com precisão o âmbito desses tratamentos[4].

9. O Projeto de Decreto-Lei em análise visa instituir um regime geral da interoperabilidade documental e de dados da Administração Pública, prevendo-se a obrigação legal das entidades públicas recorrerem à plataforma de interoperabilidade da administração pública.

10. Como adiante se analisará, o projeto de Decreto-Lei vem regular um regime de interoperabilidade que implica comunicações constantes de dados pessoais dos cidadãos sem que a norma identifique e concretize elementos essenciais do tratamento, como a delimitação clara da finalidade, as categorias de dados objeto de tratamento e entidades destinatárias de dados pessoais em cada tratamento.

11. Como se vem sublinhando em anteriores pareceres «este grau de indeterminação legislativa, numa matéria, como é a da previsão de transmissão/comunicação de dados pessoais dos cidadãos, é manifestamente contrário ao princípio da legalidade, não permitindo cumprir o grau de densidade normativa exigida à restrição de direitos, liberdades e garantias, que estas interconexões sempre representam – em especial, do direito fundamental à proteção dos dados pessoais, mas também do direito fundamental ao respeito pela vida privada, consagrados nos artigos 35.º e 26.º da Constituição da República Portuguesa (CRP).[5]

12. O Projeto de Decreto-Lei em análise visa instituir um regime geral da interoperabilidade documental e de dados da Administração Pública, prevendo-se a obrigação legal das entidades públicas recorrerem à plataforma

[3] Cf., por exemplo, o Parecer n.º 56/2017, acessível em https://www.cnpd.pt/bin/decisoes/Par/40_56_2017.pdf e o Parecer n.º 54/2018, de 15 de novembro, acessível em https://www.cnpd.pt/bin/decisoes/Par/40_54_2018.pdf.
[4] Seguimos de perto o Parecer n.º 4/2020 disponível em https://www.cnpd.pt/decisoes/historico-de-decisoes/?year=2020&type=4&ent=&pgd=2.
[5] Vide Parecer n.º 4/2020 da CNPD, disponível em https://www.cnpd.pt/decisoes/historico-de-decisoes/?year=2020&type=4&ent=&pgd=2

de interoperabilidade da administração pública gerida pela Agência para a Reforma Tecnológica do Estado, I.P. (ARTE, I.P.) e revogando o anterior desenho baseado no consentimento do cidadão (artigo 28.º-A do DL 135/99 e RCM 42/2015).

13. Ora o facto de tal plataforma centralizar fluxos de dados entre a quase totalidade das entidades públicas permitindo a identificação cruzada e exaustiva do cidadão através da informação por esta detida, causa preocupação acrescida não só quanto ao direito à proteção de dados pessoais, mas também quanto à sua compatibilidade com outros preceitos constitucionais, e, em particular com o consagrado no artigo 35.º da CRP.

14. É *inegável que a generalização de acessos recíprocos à informação constante de bases de dados na posse de entidades públicas, e de algumas entidades privadas, implica riscos para os direitos, liberdades e garantias dos cidadãos. Em causa estão os riscos associados à possibilidade de facto de inter-relacionamento de toda a informação relativa a cada cidadão*[6]*, individualizado, os quais não impactam apenas na sua privacidade (restringindo-a), como também na sua liberdade e na liberdade de desenvolvimento da sua personalidade (restringindo-as ou condicionando-as), constitucionalmente reconhecidas a cada cidadão*[7].

15. Tal preocupação encontra igualmente eco na jurisprudência do Tribunal de Justiça da União Europeia, designadamente no Acórdão Digital Rights Ireland, no qual se sublinhou que regimes de conservação e tratamento massivo e indiferenciado de dados pessoais podem afetar de modo particularmente grave os direitos fundamentais à vida privada e à proteção de dados pessoais, exigindo-se, por isso, limites claros, previsíveis e estritamente proporcionais.

16. Da análise sistemática do articulado do Projeto de Decreto-Lei, ponderada à luz da Constituição da República Portuguesa (em especial o artigo 35.º), do Regulamento (UE) 2016/679 (RGPD), da Lei n.º 58/2019, de 18 de agosto (LERGPD), do quadro europeu da interoperabilidade (Regulamentos (UE) 2018/1724 e 2024/903), e de jurisprudência do TJUE, e do Tribunal Constitucional, ressaltam algumas questões que urge analisar. Vejamos:

[6] Como em anteriores Pareceres, a CNPD tem destacado, nesta teia interligada de bases de dados, a partir de um qualquer elemento identificativo – *v.g.*, o número de identificação civil, o número de identificação fiscal ou o endereço eletrónico – pode relacionar-se toda a informação relativa a cada cidadão na posse da Administração Pública portuguesa e, inclusive, das entidades privadas abrangidas por tais disposições.
[7] E seguindo de perto a posição da CNPD já expressa no seu Parecer/2022/98.

17. Importa, antes de mais, comentar a afirmação constante no preâmbulo do projeto de diploma por traduzir um juízo incompleto sobre a finalidade do mesmo: *«Ainda que a concretização da interoperabilidade respeite apenas à modificação do mecanismo técnico de partilha da documentação – e não às atividades de tratamento conduzidas por cada entidade pública e que efetivamente impactam os titulares dos dados – entendeu o Governo que é prudente a previsão de mecanismos específicos de transparência favoráveis aos titulares dos dados e que empoderam o exercício dos respetivos direitos.»*.

18. Ora, à luz do artigo 4.º, n.º 2, do RGPD, a transmissão, divulgação por transmissão e interconexão são, todas elas, operações de tratamento autónomas e juridicamente relevantes. A transmissão de dados entre autoridades públicas constitui um tratamento de dados pessoais que exige respeito pelos princípios de tratamento de dados consagrados no artigo 5.º do RGPD, alicerçada numa base jurídica própria, específica e previsível, bem como a existência de um dever de informação autónomo ao titular dos dados.

19. Assim, não se compreende tal afirmação porquanto a aprovação do instrumento legal em análise visa precisamente constituir-se como fundamento de licitude para os tratamentos de dados resultantes da sua aplicação. Assiste-se, de facto, a uma mudança de paradigma abandonando-se o consentimento do titular dos dados pretendendo-se agora reconduzir a licitude desses tratamentos ao disposto na alínea c) do n.º 1 do artigo 6.º RGPD.

20. Embora se congratule com a constatação do que já vem sido defendido pela CNPD, isto é, no contexto em apreço o consentimento não constitui fundamento de licitude bastante, por o titular não ser verdadeiramente livre para o prestar, entendimento alicerçado no Considerando n.º 43 do RGPD e nas Diretrizes n.º 05/2020 relativas ao consentimento, na aceção do Regulamento 2016/679, adotadas pelo Comité Europeu de Proteção de Dados, em 4 de maio de 2020,[8] esta Comissão não pode deixar de realçar que tal mudança exige que a norma em análise deva responder a um objetivo de interesse público e ser proporcional ao objetivo legítimo prosseguido.

21. Para que tal juízo de proporcionalidade seja possível é fundamental que o diploma contenha e regule os aspetos essenciais do regime jurídico dos tratamentos de dados pessoais resultantes da sua aplicação.

22. Note-se que a finalidade do tratamento é determinada com esse fundamento jurídico, podendo este prever disposições específicas para adaptar a aplicação das regras do RGPD.

[8] Disponíveis em https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_pt.pdf

23. Constata-se, no entanto, que o articulado, lido em conjunto, não cumpre as demandas do artigo 6.º, n.º 3 do RGPD, que impõe que a base legal especifique as finalidades e os tipos de dados objeto de tratamento, categorias de titulares de dados e entidades a que os dados podem ser comunicados, prazos de conservação e medidas de salvaguarda destinadas a cumprir a legalidade e lealdade do tratamento — exigência que o projeto de Decreto-Lei desatende.

24. Ainda relativamente ao preâmbulo do projeto de Decreto-Lei importa tecer algumas considerações à afirmação aí produzida de que «A definição desta arquitetura quanto à obrigatoriedade de recorrer à partilha de dados entre entidades públicas constitui um regime especial face ao já previsto no artigo 23.º da Lei n.º 58/2019, de 18 de agosto, dispensando-se a celebração de protocolos adicionais entre e entidade fornecedora e a entidade consumidora».

25. Sendo certo que o n.º 2 do artigo 23.º da Lei 58/2019 admite que a transmissão de dados entre entidades públicas pode ser realizada para finalidades diferentes das que justificaram a recolha dos dados, não pode deixar de se sublinhar que *«[…] tem natureza excecional e deve ser devidamente fundamentada»* com vista a assegurar a prossecução do interesse público que de outra forma não possa ser acautelado, nos termos da alínea e) do n.º 1, e do n.º 4, ambos do artigo 6.º, e da alínea g) do n.º 2 do artigo 9.º, todos do RGPD.

26. Note-se que o RGPD regula a reutilização de dados pessoais para finalidades diferentes das que justificaram a sua recolha no n.º 4 do artigo 6.º, e desse preceito resulta, desde logo, que podem existir disposições de direito nacional ou da União a prever essa reutilização dos dados, mas apenas «[…] *se constituírem uma medida necessária e proporcionada numa sociedade democrática para salvaguardar os objetivos referidos no artigo 23.º, n.º 1, do RGPD*».

27. A CNPD já se pronunciou sobre as dificuldades da aplicação desta norma na Deliberação n.º 494/2019, aprovada em 3 de setembro de 2019[9], considerando que os fundamentos aí expressos são reconduzíveis ao diploma em análise, pelo que se remete a argumentação para o então explanado. Não pode, porém, deixar de se sublinhar, a enorme dificuldade em ver cumprido o princípio da limitação das finalidades estando em causa a reutilização de dados para finalidades diferente, transcrevendo as considerações feitas na referida Deliberação, por se manterem apertinentes e atuais: *«Acrescente-se ainda que esta norma, ao admitir que os dados pessoais podem ser tratados por entidades públicas para qualquer finalidade distinta da originária, contraria o princípio da finalidade ou da limitação das finalidades, explicitado na alínea b) do n.º 1 do artigo 5.º do RGPD – e, desde logo, consagrado no n.º 2 do artigo 8.º da Carta dos Direitos Fundamentais da União Europeia, bem como na alínea b)*

[9] Disponível em https://www.cnpd.pt/decisoes/historico-de-decisoes/?year=2019&type=2&ent=

do artigo 5.º da Convenção 108 do Conselho da Europa –, por afastar o juízo concreto e ponderado de compatibilidade das finalidades. Note-se que a exigência de fundamentação a que se reporta o n.º 1 do artigo 23.º da Lei não está imputada a tal juízo, antes parecendo referir-se à impossibilidade de acautelar o interesse público de outra forma».

28. Debruçando-nos agora sobre o articulado do Projeto de Decreto-Lei em análise verifica-se que o objeto deste diploma é estabelecer o regime geral da interoperabilidade documental e de dados para a administração pública. Mais se afirma que *"o princípio da interoperabilidade determina que os cidadãos devem apresentar os seus dados e documentos apenas uma vez"* (cf. n.º 2). Ora tal disposição revela-se pouco clara porquanto o princípio *"apenas uma vez"* (*once only*) não constitui, na verdade, um dever do cidadão, mas antes traduz uma proibição à Administração de exigir documentação que já detém, parecendo obrigar o cidadão à apresentação de documentos apenas uma única vez.

29. Por sua vez, o n.º 3 estabelece a obrigação de adoção de mecanismos de interoperabilidade em toda a infraestrutura tecnológica das entidades abrangidas, endereçando genericamente para o diploma ou "demais legislação aplicável". Tal formulação vaga, sem indicação da legislação em causa, não permite uma concreta aferição material do mecanismo que se está a propor, o que, afetando tratamentos de dados pessoais, não permite um crivo concreto de aferição crítica. Recomenda-se a reformulação deste inciso especificando e delimitando a legislação a convocar.

30. O artigo 2.º procede à definição de conceitos essenciais à cabal compreensão e aplicação do diploma, a saber a definição de dado, documento, entidade fornecedora e consumidora, plataforma de interoperabilidade da administração pública, serviço conexo e profissional liberal com profissão regulada.

31. Entende-se, no entanto, que seria importante consagrar ainda a definição de "interoperabilidade" especificando as suas diversas dimensões (organizativa, semântica, técnica ou no tempo), à semelhança do que sucede noutros instrumentos jurídicos de países europeus desta natureza[10]. Tal clarificação de conceitos é essencial para a compreensão do verdadeiro alcance do diploma e exigida por razões de clareza e segurança jurídica.

32. De igual forma se recomenda a definição de "serviço público", na medida em que constituiu uma categoria nuclear de todo o âmbito objetivo (artigos 3.º e 4.º), e cuja delimitação, embora possa ser remetida

6. Vide, por exemplo, o Real Decreto 4/20210, de 8 de janeiro, que regula o Esquema Nacional de Interoperabilidade no âmbito da Administração Eletrónica em Espanha disponível em https://www.boe.es/buscar/act.php?id=BOE-A-2010-1331

implicitamente para o conceito clássico de direito administrativo, carecerá de precisão neste contexto, por conter com o âmbito de extensão normativa.

33. Por sua vez, a definição de *"documento"* [al. b)] inclui *"qualquer representação com suporte físico e/ou digital de dados, produzidos por uma entidade abrangida ou que esteja na posse ou seja detida em nome de entidades abrangidas"*. A formulação apresenta-se demasiado ampla, permitindo abranger documentos privados sujeitos a diferentes graus de proteção (p. ex., relatórios médicos juntos a processos administrativos, correspondência privada constante de processos disciplinares, pareceres particulares), com consequências relevantes em sede do artigo 35.º, n.º 4, da CRP e ou do regime do segredo profissional. Recomenda-se assim a reformulação da mesma, por forma a se restringir aos documentos emitidos pela Administração ou para esta destinados em virtude de obrigação legal, com finalidades específicas e explícitas.

34. O âmbito de aplicação subjetivo do Projeto de Decreto-Lei inclui todos os órgãos e serviços da administração direta do Estado, todas as entidades da administração indireta, entidades administrativas independentes, autarquias locais, entidades empresariais pertencentes ao setor empresarial do Estado ou ao setor empresarial local nos termos do artigo 5.º do Decreto-Lei n.º 133/2013, de 3 de outubro, estendendo-se às regiões autónomas.

35. Uma nota ainda quanto ao n.º 4 deste inciso — exclusão das entidades quando atuem em "*atividade de cariz industrial ou comercial, sem ligação aos serviços públicos que prestam*" — sublinhando que a norma é tecnicamente vaga, na medida em que assenta apenas no critério *"sem ligação aos serviços públicos"* podendo potencialmente originar problemas interpretativos na delimitação do seu âmbito de aplicação[11].

36. Assim, seria desejável e útil a reformulação desta alínea por forma a concretizar, de forma clara, os critérios de exclusão de entidades do âmbito de aplicação subjetivo, uma vez que tal exclusão tem implicações diretas para quem está abrangido pelo diploma e, bem assim, nos tratamentos que este pressupõe.

37. Acresce que no n.º 3 do artigo 4.º se excluem da obrigatoriedade de recorrer à interoperabilidade através da plataforma de interoperabilidade da Administração Pública as forças e serviços de segurança, entidades reguladoras e entidades de fiscalização, com referência ao referido "serviço público". Alerta-se para o facto de a utilização deste conceito aberto poder levantar dificuldades quando confrontado com o regime instituído pela Lei n.º 59/2019, de 8 de agosto, que transpõe a Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 20216. Isto é, o diploma é claro quanto à possibilidade das forças e serviços de segurança atuarem como entidades consumidoras relativamente aos serviços públicos prestados no âmbito das alíneas a)

[11] Veja-se por exemplo o caso das Entidades Públicas Empresarias.

e b) do n.º 1 do artigo 4.º, mas o Projeto de Decreto-Lei não esclarece qual o regime aplicável quando consomem dados oriundos de tratamentos sujeitos ao RGPD, ou tratados com fins de repressão e investigação, ou referentes a condenações ou infrações penais (10º RGPD), nem ainda como se assegura a separação de finalidades.

38. Quanto ao âmbito objetivo previsto no artigo 4.º do Projeto de Decreto-Lei refira-se que a formulação do n.º 1 se traduz numa abrangência geral dos serviços iniciados por particular, no contexto de procedimento administrativo de iniciativa particular ou iniciados pela Administração nos termos da lei. Este âmbito tão amplo de abrangência levanta preocupações acrescidas do ponto de vista regime da proteção de dados pessoais na medida que o universo de informação tratada se destinará a uma multiplicidade de fins não definidos não se encontrando densificado o motivo para tal.

39. Acresce que o n.º 5 daquele mesmo preceito legal prevê que dados *"alojados em plataformas detidas por outras entidades que não as abrangidas"* sejam disponibilizados através da plataforma de iAP. Tal implica que a disponibilização possa abranger dados alojados em prestadores privados (designadamente *cloud providers*), com obrigações de partilha que podem entrar em conflito com contratos privados, ou regimes especiais de proteção de dados. A norma não esclarece se a obrigação de "partilhar com a entidade fornecedora" implica nova transmissão de dados (e, portanto, novo tratamento, com novas exigências previstas no n.º 3 do artigo 6.º do RGPD), nem identifica a base de licitude dessa transmissão prévia. Sugere-se revisitação da norma com vista à sua clarificação.

40. Uma nota apenas para o facto de o n.º 6 artigo 4.º do Projeto de Decreto-Lei fazer remissão para o artigo 14.º — dados pessoais de categorias especiais e sujeitos a sigilo – certamente por lapso, pretendendo-se eventualmente referir o artigo 16.º - partilha com entidades não abrangidas.

41. Passando agora à análise do âmbito de aplicação territorial – artigo 5.º do Projeto de Decreto-Lei - a norma limita-se a referir que a aplicação do disposto no diploma a entidades abrangidas localizadas em países terceiros depende da verificação dos requisitos aplicáveis às transferências internacionais de dados. Tal disposição revela-se manifestamente insuficiente porquanto se limita a remeter para o regime legal previsto no capítulo V do RGPD (artigos 44.º a 50.º) não concretizando nenhum dos seus fundamentos. Vejamos:

42. Só são permitidas transferências internacionais de dados pessoais para países terceiros ou organizações internacionais se ocorrerem com base numa decisão de adequação emitida pela Comissão Europeia ou na ausência de tal decisão se os responsáveis pelo tratamento ou subcontratantes tiverem apresentado garantias adequadas e na condição dos titulares dos dados gozarem de direitos oponíveis e de medidas jurídicas corretivas

eficazes. Tais garantias podem ser previstas por qualquer dos meios previstos nas alíneas a) a f) do n.º 2 do artigo 46.º do RGPD ou por meio de cláusulas contratuais ou disposições a inserir nos acordos administrativos entre autoridades ou organismos públicos que contemplem os direitos efetivos e oponíveis dos titulares dos dados, sob reserva de autorização da autoridade de controlo. O artigo 49.º do RGPD prevê ainda derrogações para situações específicas.

43. Importa, pois, que no articulado conste a identificação da base legal de suporte às transferências internacionais de dados a realizar no âmbito do presente diploma, as salvaguardas adicionais que lhe correspondem, ou os mecanismos de avaliação prévia.

44. Neste domínio assume particular relevância a jurisprudência do Tribunal de Justiça da União Europeia resultante do Acórdão Schrems II, onde se reafirmou que as transferências internacionais de dados pessoais apenas são admissíveis quando o nível de proteção assegurado no país terceiro seja substancialmente equivalente ao garantido no espaço da União Europeia, exigindo-se mecanismos efetivos de controlo e salvaguardas adequadas.

45. Estranha-se, por isso, a opção enunciada no n.º 2 do artigo 5.º do projeto de Decreto-Lei, que prevê a exclusão *"por portaria do membro do Governo responsável pelos negócios estrangeiros das entidades abrangidas que se localizem nos países que se entenda não garantirem condições de segurança adequadas para a aplicação segura da interoperabilidade"*, porquanto a apreciação dessa adequação é da competência da Comissão Europeia, tomada após uma análise exaustiva dos elementos constantes no n.º 2 do artigo 45.º do RGPD, após emissão de Parecer por parte do Comité Europeu de Proteção de Dados. Ora uma norma que atribui tal competência ao membro do Governo responsável pelos negócios estrangeiros, despida de critérios objetivos para a apreciação da segurança adequada para a aplicação da interoperabilidade, parece introduzir um juízo discricionário, sem qualquer balizamento normativo, contrariando o regime consagrado no quadro jurídico europeu sobre tal matéria e conflituando com a competência da Comissão Europeia para apreciar a adequação ao abrigo do artigo 45.º RGPD e as suas vinculações e efeitos.

46. Além de que parece contrastar com o regime previsto no artigo 10.º, n.º 4, aplicável apenas à ARTE, IP, (transferências admitidas apenas para países com decisão de adequação), gerando incoerência entre o âmbito territorial geral e o da entidade subcontratante.

47. Quanto ao artigo 6.º do Projeto de Decreto-Lei (Catálogo Único dos Serviços Públicos) refira-se que este Catálogo Único parece ser desenhado como instrumento de transparência. Contudo, o catálogo não substitui — não pode substituir — a medida legislativa exigida pelo artigo 6.º, n.º 3, do RGPD onde se consagra que a base

legal deve, ela própria, definir as finalidades do tratamento de uma forma clara e precisa. A mera remissão para instrumento administrativo (o catálogo) não poderá substituir a medida legislativa com o conteúdo exigido.

48. Faz-se notar a ausência de previsão no articulado das exigências consagradas nos artigos 13.º e 14.º do RGPD (informação ao titular), nomeadamente de uma eventual articulação entre a obrigação de registo no Catálogo Único de Serviços Públicos pelas entidades abrangidas da identificação dos dados e documentos necessários à execução dos serviços que prestam, bem como das entidades detentoras desses elementos, e os deveres de transparência das entidades responsáveis, ou a sua reserva. Recomenda-se a densificação da obrigação de informação ao titular de dados nos termos previstos no considerando 39 e artigos 13.º e 14.º do RGPD.

49. O n.º 2 do artigo 7.º do Projeto de Decreto-Lei dispõe que *"as entidades fornecedoras devem aderir à referida plataforma, disponibilizando o acesso a toda a documentação e dados que produzem na prestação dos seus serviços ou no decurso da sua atividade"*.

50. Esta formulação consagra uma lógica de partilha, por defeito, da totalidade da informação, oposta ao princípio da minimização de dados consagrado no artigo 5.º, n.º 1, alínea c), e ao princípio da proteção de dados por defeito plasmado no n.º 2 do artigo 25.º, ambos do RGPD. Recomenda-se a reformulação deste inciso por forma a conter, pelo menos, uma especificação da informação em causa por tipologias documentais, disposições relativas à granularidade de acesso (que atributo? hit/no hit? documento completo?) bem como especificação de limitações de acesso à entidade consumidora concretamente autorizada para o serviço.

51. Sublinha-se que a transmissão deve limitar-se ao estritamente necessário, preferindo-se, sempre que possível, a mera confirmação de atributos ou estados em vez da transmissão integral dos dados.

52. Por sua vez, o n.º 6 do artigo 7.º do Projeto dispensa a *"celebração de quaisquer protocolos adicionais"*. A ausência completa de instrumento documental entre fornecedor e consumidor esbarra com a responsabilidade do responsável (artigo 5.º, n.º 2, RGPD) e o regime de responsabilidade entre eles, ou de regime de tratamento de dados e sua proteção. Estamos perante uma norma utilizando uma formulação aberta que tudo permite, ignorando por completo o regime jurídico de proteção de dados pessoais. Caso a opção legislativa seja efetivamente dispensar protocolos, o regime devia exigir um padrão, identificando para cada fluxo a base legal, finalidade, tipos de dados, prazos e medidas de segurança.

53. Note-se ainda que a dispensa da celebração de protocolos não deve ser interpretada como dispensa da contratualização das responsabilidades entre os responsáveis do tratamento de dados pessoais. Deve sempre

ser garantido o princípio da responsabilização. Essa responsabilização pode ser agilizada pela aceitação de um termo de responsabilidade.

54. Sugere-se a adoção de medidas mitigadoras para o risco de acessos massivos que não cumpram os princípios da minimização de dados. Essas medidas passarão por monitorização do uso por entidade consumidora de dados e auditoria e rastreio para aferir indiretamente o grau de proporcionalidade entre os pedidos de dados efetuados e os pedidos efetivamente espoletados por iniciativa particular ou por atribuição legal da entidade que solicitou os dados.

55. Não obstante ser louvável a intenção vertida no n.º 7 do artigo 7.º, que consagra a obrigatoriedade de a disponibilização de informação ocorrer a partir da sua fonte primária ou autêntica, e das garantias de minimização estipuladas nos n.ºs 2 e 5 do artigo 8.º, que restringem a transmissão aos dados "estritamente necessários", considera-se tecnicamente imperativo que o artigo 8.º materialize uma proibição expressa de utilização da plataforma de interoperabilidade para a realização de cópias massivas ou integrais de bases de dados (data dumping).

56. A ausência de uma interdição clara à criação de réplicas locais de informação detida por terceiras entidades viabiliza um desvio de finalidade sistemático, em que a plataforma deixa de ser um canal de consulta pontual e instrumental para a prestação de um serviço específico para se tornar num veículo de alimentação de bases de dados paralelas. Esta prática, para além de acarretar o risco iminente de sobrecarga na infraestrutura e eventual colapso da disponibilidade dos sistemas da ARTE, I.P., colide frontalmente com os pilares do RGPD.

57. Relativamente ao artigo 8.º (Minimização dos dados) importa referir, antes de mais, que a operacionalização do n.º 3 ("sempre que tecnicamente viável") depende da arquitetura da plataforma, que o projeto de Decreto-Lei não regula tecnicamente. Estando em causa matéria de direitos fundamentais mal se compreende a formulação atual da norma, sujeitando a sua proteção às especificidades tecnológicas existentes em detrimento da promoção de uma solução que responda à proteção efetiva desses direitos.

58. Por sua vez, o n.º 5 admite, salvo "exceções decorrentes de alteração do serviço público", a solicitação de dados adicionais. Mais uma vez o legislador recorre a normas abertas não concretizando o tipo de exceções em causa, sendo por isso potencialmente permissiva em relação à proteção de dados pessoais. Recomenda-se, pois, um mínimo de especificação das possíveis exceções por forma a evitar a garantir a proteção deste direito fundamental.

59. Ainda sobre a minimização de dados, é desejável que venham a existir mecanismos de proteção contra a exfiltração massiva de dados, caso haja comprometimento do acesso à plataforma iAP na infraestrutura tecnológica do fornecedor ou consumidor de dados.

60. Por fim, sublinha-se a ausência de referências normativas relativas a eventuais agregações ilícitas. O princípio da minimização de dados exige não apenas limitar o pedido de informação ao estritamente necessário para a finalidade prosseguida, mas, como consequência, também proteger ou impedir que se reconstrua, por agregação, perfil mais amplo do que o autorizado.

61. Também a jurisprudência do Tribunal de Justiça da União Europeia tem vindo a salientar os riscos associados à agregação e interconexão de informação pessoal em larga escala, sublinhando-se, no Acórdão *La Quadrature du Net*, a especial gravidade de mecanismos suscetíveis de permitir a reconstituição transversal da vida privada dos cidadãos através do cruzamento de múltiplas categorias de dados.

62. Debrucemo-nos agora sobre o artigo 9.º do Projeto de Decreto-Lei (Responsabilidade pelo tratamento), cujo n.º 2 dispõe: *"A entidade fornecedora não pode, em qualquer caso, ser responsabilizada pela utilização abusiva que seja realizada pela entidade consumidora."* Esta cláusula suscita algumas questões jurídicas, desde logo, por poder conflituar com o artigo 82.º, n.º 2 e n.º 4, do RGPD, que consagram, respetivamente, que *"Qualquer responsável pelo tratamento que esteja envolvido no tratamento é responsável pelos danos causados por um tratamento que viole o presente regulamento."*, e consagram ainda uma solidariedade entre responsáveis envolvidos no mesmo tratamento, *"a fim de assegurar a efetiva indemnização do titular dos dados"*. Uma norma nacional não se afigura passível de poder eliminar essa solidariedade, sob pena de violar a o primado do Direito da União Europeia.

63. Pense-se, desde logo, em situações em que a entidade fornecedora pode ter responsabilidade autónoma por falhas na verificação da legitimidade do pedido, no controlo de acesso, ou de violação do dever de informação prévio, para se questionar o sentido de tal disposição.

64. Por sua vez, salienta-se que o n.º 3 do artigo 9.º do Projeto de Decreto-Lei se limita a recordar o dever de informação, sem definir como se articulam os deveres das diversas entidades envolvidas. Urge, pois, fixar no diploma os procedimentos necessários à efetiva prestação destes deveres.

65. Por último recorda-se que as responsabilidades são atribuídas aos papéis de entidade fornecedora e entidade consumidora. Como já referido no presente parecer, estes papéis e responsabilização inerente devem ser contratualizados, no mínimo pela adesão à plataforma de interoperabilidade através de um termo de responsabilidade.

66. Nos termos do disposto no artigo 10.º do Projeto de Decreto-Lei, a ARTE, I.P. assume o papel de subcontratante. Não se pondo em causa a atribuição da qualidade de subcontratante, sempre se dirá que a figura da autorização *ope legis* universal contraria a literalidade e a teleologia do artigo 28.º, n.º 2 do RGPD, uma vez que o responsável (entidade aderente) não é informado, não pode opor-se e não tem possibilidade de exercer controlo efetivo sobre a sua atividade.

67. Neste quadro assume especial importância o conteúdo obrigatório do ato legal que regule a subcontratação (uma vez que a lei não distingue, nesse caso, contrato de ato normativo) recordando-se que deverá preencher o exigido pelo n.º 3 do artigo 28.º, do RGPD. Assim, deve conter todos os elementos nele taxativamente previstos: o objeto e duração do tratamento, a sua natureza e finalidade, o tipo de dados pessoais e as categorias dos titulares dos dados, as obrigações e os direitos do responsável pelo tratamento. Constata-se, porém, que o artigo 10.º do projeto é omisso, desde logo, quanto à identificação clara da natureza e finalidade do tratamento por tipologia, omisso quanto à identificação dos tipos de dados pessoais a tratar e ainda quanto às categorias de titulares abrangidos. Recomenda-se a reformulação do artigo 10.º por forma a prever estes elementos em falta.

68. Note-se que o n.º 8 deste artigo contem a única referência à realização de avaliações de impacto sobre a proteção de dados pessoais (AIPD). Salienta-se que a decisão de elaboração, ou não, de uma AIPD deriva da avaliação do risco que o tratamento de dados comporta para os direitos dos titulares dos dados. Deve, portanto, ser equacionada a obrigatoriedade da avaliação do risco na direta proporcionalidade do grau de concentração de dados a que uma entidade recetora terá acesso.

69. Sobre a notificação de violação de dados regulada no n.º 9 constata-se não existir qualquer referência à obrigação de notificar os titulares de dados, consagrada no artigo 34.º RGPD, sempre que a violação de dados pessoais for suscetível de implicar um elevado risco para os direitos e liberdades de pessoas singulares. Recomenda-se, pois, a inclusão de tal obrigação no artigo 10.º do Projeto de Decreto-Lei.

70. Estranha-se o conteúdo do n.º 10 deste artigo que dispõe que "Caso em algum momento a ARTE, IP, venha a ter acesso a dados pessoais transmitidos entre as entidades públicas, deve eliminá-los imediatamente e, em qualquer caso, quando cessar a subcontratação aqui referida deve eliminá-los ou devolve-los ao respetivo responsável pelo tratamento, de acordo com a escolha do mesmo". Ora a norma parte da premissa de que a ARTE, IP, não acede aos dados pessoais, mas prevê a possibilidade de vir a aceder, o que é, no mínimo, contraditório e poderá configurar uma situação que tipifica uma violação de dados pessoais ou um tratamento ilícito de dados. Assim sendo, não se alcança a razão pela qual a lei consagra a obrigatoriedade de os eliminar.

71. Acresce que a configuração tecnológica deve evidenciar a impossibilidade material de acesso, pelo que essa configuração deve ser objeto de obrigação legal expressa. Recomenda-se assim, a alteração do texto por forma a consagrar tal obrigação.

72. O n.º 11 do artigo trata dos registos obrigatórios quanto à documentação e aos dados transmitidos através da plataforma iAP fixando um prazo de 3 anos para a sua conservação sem, no entanto, ser dada qualquer fundamentação para a exigência desse prazo. Urge, assim proceder à fundamentação do prazo fixado.

73. Questão mais complexa é a suscitada pela definição da finalidade de tratamento prevista no artigo 11.º do projeto de Decreto-Lei que a reconduz à *"prestação do serviço público referido no artigo 4.º, ou de serviço conexo"*, entendendo-se este como serviço público que, sendo relacionado ou decorrente de um dos serviços descritos no n.º 1 do artigo 3.º, são opcionais para o cidadão – cf. alínea f) do artigo 2.º).

74. Sendo certo que, nos casos em que o tratamento de dados seja realizado em conformidade com uma obrigação jurídica à qual esteja sujeito o responsável pelo tratamento, cabe ao direito da União ou dos Estados-Membros determinar qual a finalidade do tratamento dos dados (cf. considerando 45 do RGPD) a opção do legislador recorrer a uma cláusula geral, conflitua desde logo com o princípio da limitação das finalidades constante no artigo 5.º, n.º 1, alínea b), do RGPD, que exige finalidades *"determinadas, explícitas e legítimas"*.

75. Tal opção parece ainda contender com o artigo 6.º, n.º 3, do RGPD, na medida em que aqui se reclama que essa base legal defina as finalidades do tratamento de dados a efetuar, exigindo-se clareza quanto à natureza, ao alcance e à duração dos tratamentos, aos motivos, às autoridades competentes e aos direitos dos titulares dos dados, em cada caso, disponíveis.

76. Insiste-se, uma leitura atenta da primeira parte do n.º 3 do artigo 6.º permite concluir que a lei tem, pelo menos, de definir a finalidade do tratamento, pelo que a indicação vaga de uma finalidade retira qualquer força de fonte legitimadora do tratamento de dados pessoais para finalidades diferentes.

77. Note-se ainda que a norma falha em identificar, com a especificidade exigida, os tipos de dados objeto de tratamento, as categorias de titulares envolvidas, os destinatários específicos ou categorias de destinatários por fluxo ou pedidos, as finalidades específicas para cada tipologia de serviço a prestar e os prazos de conservação aplicáveis ao tratamento posterior.

78. Ainda que se argumente que a identificação de alguns desses elementos se encontra registada no Catálogo Único dos Serviços Públicos, nos termos do artigo 6.º do projeto de Decreto-Lei, sempre se dirá tratar-se de um mero registo administrativo incapaz de se substituir à medida legislativa exigida como fundamento jurídico do tratamento de dados.

79. Por se entender ser a questão da finalidade do tratamento essencial na determinação da legalidade do mesmo, a CNPD entende que a norma em análise não cumpre minimamente o regime jurídico de proteção de dados pessoais, nomeadamente o principio da finalidade do tratamento nem as exigências impostas no n.º 3 do artigo 6.º do RGPD, pelo que deve ser totalmente reformulada sob pena de a mesma não se constituir com o instrumento jurídico valido do fundamento de licitude previsto na alínea c) do n.º 1 do artigo 6.º do RGPD.

80. Por sua vez, o artigo 12.º do Projeto de Decreto-Lei tem como epígrafe *«Direitos dos titulares dos dados»*. Aqui se dispõe que a interoperabilidade é feita em condições de *"segurança, confiança, confidencialidade e rastreabilidade"*. Tal disposição tem natureza meramente programática nada acrescentando às obrigações previstas no artigo 32.º RGPD, relativo á segurança do tratamento.

81. A CNPD destaca que todas as operações de tratamento de dados deverão cumprir os princípios da integridade e confidencialidade - bem como o da responsabilidade - e, portanto, *"tratados de uma forma que garanta a sua segurança, incluindo contra o seu tratamento não autorizado ou ilícito e conta a sua perda, destruição ou danificação acidental, adotando medidas técnicas ou organizativas adequadas"*[12].

82. Quanto a esta matéria, a CNPD emitiu, já, orientações para as organizações sobre medidas de segurança que devem ser adotadas para minimizar as consequências para os direitos das pessoas, aprovando a Diretriz 2023/1, para aí se remetendo na íntegra.

83. Transcreve-se aqui o disposto no nosso Parecer/2024/59:

> *«82. Mas, relembre-se, ao não se definirem na Lei os termos e um pleno regime de proteção de dados, que justificam os tratamentos e consolidam como serão feitos, impossibilita-se uma análise concreta e concatenada, a realizar-se com referência aos princípios axiológicos e práticos que estes têm de cumprir.*
> *83. Ademais, a concentração de informação dos dados pessoais dos cidadãos em bases de dados que não se constituam desse modo, acrescidas de fluxos, acessos e interconexões por sujeitos vários, faz aumentar exponencialmente o risco de violação de dados pessoais ou fugas de informação ao longo da cadeia, e cuja identificação, reparação ou domínio se podem revelar incontroláveis, por incontidas quer no seu acesso, quer nos destinatários, e que deve estar cada vez mais presente na mens legislatoris, logo na formulação dos seus comandos, obstando, na medida do possível, a essas oportunidades*[13]*.»*

[12] Cfr., a este propósito, o artigo 5.º do RGPD. Este inciso deverá ser complementado em articulação com o artigo 4.º, n.º 12 do RGPD, bem como os artigos 25.º e 32.º também deste Regulamento.
[13] A minimização destes riscos não se remete somente a execuções ou aspetos técnico-informáticos, mas também nas estruturas de tratamento que as normas determinam.

84. O n.º 2 do artigo 12.º do Projeto de Decreto-Lei atribui a cada uma das entidades envolvidas nos tratamentos de dados, a obrigação de assegurar o exercício dos direitos dos titulares nos termos e com *"as limitações previstas no Regulamento Geral sobre a Proteção de Dados"*.

85. Ora, as limitações ao exercício de direitos estão previstas no artigo 23.º do RGPD, exigindo uma medida legislativa específica, que respeite o conteúdo essencial dos direitos e liberdades fundamentais e constitua uma medida necessária e proporcionada para assegurar os objetivos elencados nas diversas alíneas do n.º 1. Só nestas circunstâncias, poderá ocorrer limitação de direitos dos titulares, sem que as entidades envolvidas no tratamento tenham qualquer poder determinativo da extensão dessa limitação.

86. Saúda-se a obrigatoriedade de conservação da informação sobre as ações realizadas por meio da plataforma iAP (*logs*) prevista no n.º 3. Porém, nota-se que tal regime deve ser articulado com o exercício dos direitos dos titulares de dados, desde logo, o direito de acesso, permitindo ao titular saber a que entidades concretas os seus dados foram transmitidos via plataforma. O histórico dos tratamentos de dados poderá ser obtido através dos registos referidos (*logs*) mas importa concretizar o exercício efetivo dos direitos dos titulares.

87. Assim, a CNPD recomenda que se positive no texto em análise a forma de concretização efetiva dos direitos dos titulares, à semelhança do que acontece noutros normativos (vide por exe o n.º 6 do artigo 29.º da Lei n.º 58/2029 no que respeita aos dados de saúde).

88. Para a concretização prática e operacional do direito referido no ponto anterior, propõe-se a criação de um portal de transparência integrado na plataforma iAP. Este portal funcionará como a interface oficial de acesso para os cidadãos, disponibilizando um *dashboard* que permita não só consultar o histórico detalhado de acessos (com base nos *logs* conservados), mas também gerir perfis de acesso e consentimentos granulares de forma ágil e segura.

89. Além disso, o artigo revela algumas insuficiências: desde logo, é omissa relativamente à existência de um ponto de contacto ou balcão de exercício de direitos junto da ARTE, IP, sem o qual os cidadãos não podem eficazmente exercê-los. É ainda omissa quanto ao exercício do direito à informação relativo à própria interoperabilidade — devendo o titular ser informado, por exemplo, no momento da submissão do requerimento para prestação de um serviço, das entidades que serão ou poderão ser consultadas através da plataforma para a satisfação do mesmo.

90. E, por último, não cuida da articulação da repartição de funções entre entidade fornecedora e entidade consumidora com vista a facilitar o exercício de direitos do titular, e clarificando quem responde a um pedido de

acesso (artigo 15.º RGPD), quem precede à retificação dos dados (artigo 16.º); quem concretiza a eliminação ou apagamento dos mesmos (artigo 17.º).

91. O artigo 13.º consagra o princípio de que toda a documentação necessária à prestação de um serviço público pode ser entregue por canais digitais devendo ser dada prioridade a esta via sem prejuízo dos regimes legais especiais aplicáveis ao acesso de dados constantes dos sistemas de registo, designadamente do registo civil e registo da identificação civil. Alerta-se para o facto de o catálogo dos regimes especiais ser substancialmente mais vasto do que os exemplificativamente apontados, podendo alguns regimes (vide o registo criminal ou os registos profissionais) suscitar questões particulares que necessitam de ser ponderadas e legalmente enquadradas.

92. Uma nota ainda para a ausência de qualquer previsão sobre canais para pessoas com limitações no acesso digital (idosos, descapacitados, populações em zonas sem cobertura, etc), necessária para garantir o recurso em exclusivo à interoperabilidade através da plataforma de interoperabilidade da administração pública, pelo que se impõe regulamentação específica no articulado sobre esta matéria.

93. Especiais preocupações levanta o tratamento de dados pessoais de categorias especiais e sujeitos a sigilo tratado no artigo 14.º do projeto. Vejamos:

94. Pese embora o n.º 1 do artigo salvaguarde, no essencial, o regime consagrado no artigo 9.º RGPD, importa positivar a obrigação de a plataforma, por desenho, bloquear a partilha de dados enquadráveis em categorias especiais, sem a confirmação ativa da base legal específica, como decorre da aplicação do princípio da privacidade por desenho.

95. Por outro lado, o n.º 4 da norma dispõe «quando necessário, o consentimento expresso dos titulares dos dados deve, preferencialmente, ser obtido através do sistema de autorização associado à chave móvel digital, ou qualquer um que lhe suceda». Não esquecendo que se trata de categorias especiais de dados, sempre se dirá que tal disposição parece ser contraditória com o preâmbulo do projeto quando advoga que o desequilíbrio entre cidadão e Administração afasta o consentimento como base de licitude juridicamente válida para tratamentos comuns, e, consequentemente, o afasta para categorias especiais de dados onde o regime jurídico de proteção de dados é manifestamente mais exigente.

96. Acresce que a limitação preferencial ao recurso a sistema de autorização associado à chave móvel digital, prevista no n.º 4, sem indicação de alternativas, pode tornar o consentimento inacessível a parte significativa da população, podendo potencialmente violar o princípio da igualdade constitucionalmente consagrado no artigo 13.º CRP, e o princípio da acessibilidade previsto nas Lei n.º 36/2011, de 21 de junho, e Lei n.º 22/2025, de 19

de março, estando ainda em clara contradição com o disposto no Considerando 32 do RGPD. Pese embora não estarmos perante uma imposição legal, recomenda-se a previsão de alternativas ao recurso a sistemas ade autorização associados à chave móvel digital no n.º 4 do artigo 14.º do projeto de Decreto-Lei com vista a garantir o princípio da igualdade dos cidadãos.

97. Ainda relativamente ao artigo 14.º, importa salientar que para além do sigilo da administração tributária, devem ser equacionados outros regimes de sigilo profissionais e materiais que podem ser afetados pela interoperabilidade administrativa, designadamente, sigilo médico, sigilo bancário, sigilo profissional, sigilo estatístico, ou referente à identidade biológica, entre outros, face ao âmbito de aplicação subjetiva do diploma que abarca a quase totalidade dos serviços da administração pública.

98. Outro ponto sensível do projeto é relativo à partilha de dados e documentação com entidades não abrangidas, previsto no artigo 16.º, na medida em que permite a utilização da plataforma da interoperabilidade da Administração Pública a entidades privadas e a profissionais liberais com profissão regulada, mediante protocolo escrito.

99. Tal matéria deveria ser sujeita a uma avaliação de impacto sobre os riscos para os titulares dos dados, atendendo a que cada protocolo configura um novo tratamento de dados pessoais, sem qualquer referência a fundamentação detalhada de necessidade e proporcionalidade do tratamento, materializando o teste exigido pelo n.º 4 do artigo 6.º do RGPD para casos em que a finalidade do tratamento é diferente daquela para que os dados foram recolhidos.

100. Por outro lado, faz-se notar que o n.º 1 do artigo 16.º do projeto ao permitir a partilha de dados entre entidades não abrangidas, privadas ou públicas ou pessoas singulares que exerçam profissões liberais reguladas constitui uma norma legislativa aberta, inadmissível em matéria de direitos fundamentais, na medida em que não cuida de especificar quais são as entidades ou serviços privados ou públicos abrangidos nem os dados passíveis de tratamento.

101. Um tal grau de indeterminação legislativa numa matéria como é a transmissão de dados pessoais dos cidadãos na posse da administração pública é manifestamente contrário ao principio da legalidade, não permitindo cumprir o grau de densidade normativa exigida à restrição de direitos, liberdades e garantias em especial do direito fundamental à proteção de dados pessoais, mas também do direito fundamental ao respeito pela vida privada consagrados nos artigos 35.º e 26.º da CRP entendimento que a CNPD tem vindo sucessivamente a afirmar em pareceres sobre propostas legislativas.

102. Por outro lado, a remissão para protocolo regulando a interoperabilidade e comunicação de dados entre estas entidades genericamente indicadas também não é, na perspetiva da CNPD, insuficiente pelas razões expostas.

103. E, ainda, quanto à celebração de protocolos, importa relembrar que na medida em que correspondem a atos jurídicos de entidades públicas que definem regras vinculativas para as partes quanto a tratamento de dados pessoais e na medida em que tais regras afetam a esfera jurídica dos titulares dos dados pessoais objeto de tratamento, têm natureza de regulamento administrativo. Nessa medida, nos termos do n.º 4 do artigo 36.º e da alínea c) do n.º 1 do artigo 57.º do RGPD, têm de ser sujeitos a apreciação prévia da CNPD.

104. Para que não subsistam dúvidas quanto a tal dever, a CNPD recomenda a sua explicitação no texto do artigo.

105. Relativamente ao conteúdo do protocolo, tratado no n.º 2, observa-se que o mesmo deveria fixar os quadros em que os mesmos podem ser realizados, os seus objetos, e qual os elementos obrigatórios que neles tem de constar.

106. Por sua vez não se alcance o sentido do conteúdo do n.º 3. Da sua leitura parece resultar a abertura ao acesso da plataforma da iAP quando esteja em causa a prestação de "serviços ou execução de atividades de cariz público, administrativo ou judicial" prestados por privados. A formulação ampla e vaga do inciso permite uma interpretação lata, abrangendo situações de delegação, contratação ou exercício de funções públicas por privados. Mas a formulação não é clara pelo que recomenda a sua clarificação.

107. No n.º 4 admite-se novamente o consentimento do titular como fundamento de licitude do tratamento, ainda que, num contexto de relação entre titular e entidade privada, onde não se coloca o problema de desequilíbrio entre a posição do cidadão e da administração. Mas embora a questão da validade pareça resolvida, sempre se colocará a questão da sua liberdade efetiva, cuja análise reclama a ponderação das circunstâncias concretas da sua obtenção.

108. Quanto às normas técnicas da plataforma da interoperabilidade da AP o diploma nada concretiza. O mesmo se diga relativamente às medidas de segurança elencadas no artigo 17.º na medida em que se limitam a reproduzir a obrigação geral do artigo 32.º RGPD, sem as densificar.

109. Para além da adoção de regimes de pseudonimização e cifragem, a CNPD recomenda que o articulado especifique medidas técnicas concretas, como uso de protocolos de comunicação seguros (ex: TLS 1.3) e cifragem em repouso e ainda Implementação de um registo de auditoria (*logs*) imutável e acessível ao próprio

titular dos dados pessoais exigindo que cada consulta de dados gere um "log" que identifique o autor, a finalidade, a data e o fragmento de informação consultado.

110. Por último o artigo 20.º (Responsabilidade) limita-se a remeter para o regime disciplinar constante do Regime Geral do Trabalho em Funções Públicas, aprovado em anexo pela Lei n.º 35/2014, de 20 de junho (LGTFP) e no Estatuto do Pessoal Dirigente dos Serviços e Organismos da Administração Pública, aprovado pela Lei n.º 2/2004, de 15 de janeiro, não contemplando a responsabilidade da entidade pública enquanto pessoa coletiva (responsável pelo tratamento), a responsabilidade contraordenacional prevista nos artigos. 83.º RGPD e artigos. 37.º a 39.º da Lei n.º 58/2019, nem abrangendo a responsabilidade civil prevista no artigo 82.º RGPD e na Lei n.º 67/2007 (responsabilidade civil extracontratual do Estado). Sublinha-se que além da responsabilidade disciplinar consagrada na (LGTFP), em matéria de dados pessoais, subsiste um regime de responsabilidade em vigor, que também pode emergir das violações deste diploma.

111. Impõe-se uma referência à AIPD que acompanha o projeto de Decreto-Lei realçando que a mesma estabelece regras de negócio e imposição de medidas técnicas que não se aferem do texto do Projeto em si. Tais disposições, a serem de implementação obrigatória, deveriam ser transpostas para o articulado em análise, adquirindo força jurídica vinculativa. Destacam-se as previsões sobre o funcionamento detalhado do mecanismo de federação de identidades assente em tokens opacos (apenas decifráveis pelas entidades finais) para impedir que a ARTE, I.P. correlacione pedidos ou identifique diretamente o titular; a proibição técnica de interrelação de bases de dados através de identificadores únicos (em cumprimento do Art. 35.º, n.º 5 da CRP); a especificação de medidas de segurança granulares como o uso de EDR/EPS em sistemas operativos, autenticação multifator (MFA) obrigatória no *backoffice* e a gestão de encriptação de *endpoints*; e, por fim, a clarificação de que os registos de auditoria (*logs*) conservados pela plataforma não permitem a identificação dos titulares afetados pela transmissão de informação, garantindo uma camada de privacidade por desenho que o texto legislativo apenas enuncia de forma genérica.

III. Conclusão

112. Da análise do Projeto de Decreto-Lei ressalta o recurso pelo legislador nacional a normas abertas ou de formulação vaga com diretas implicações no regime de proteção de dados pessoais, sendo manifestamente contrário ao princípio da legalidade e impossibilitando um juízo crítico sobre o regime jurídico que se pretende instituir. Nesse sentido a CNPD recomenda a revisitação das mesmas por forma a conferir-lhe a densidade normativa que o regime dos direitos fundamentais reclama, a par da adoção da forma legal correta (Proposta de Lei a apresentar à Assembleia da República, ou Proposta de Lei de Autorização também a apresentar à Assembleia da República – artigo 165.º, n.º 1, alínea b) da CRP).

113. Quanto a disposições concretas do diploma, nos termos e com os fundamentos supra referidos a CNPD recomenda:

a) A densificação da legislação em causa referida no n.º 3 do artigo 1.º;

b) A inclusão no artigo 2.º de definição de «interoperabilidade», de «serviço público» e a clarificação do conceito de «documento» nos termos expostos nos pontos 31 a 36;

c) A reformulação do n.º 4 do artigo 3.º por forma a concretizar, de forma clara, os critérios de exclusão de entidades do âmbito de aplicação subjetivo;

d) A clarificação do n.º 3 do artigo 4.º na parte que concerne à exclusão da obrigatoriedade de utilizar a plataforma iAP por parte das forças e serviços de segurança;

e) Relativamente ao n.º 5 do artigo 4.º a revisitação da norma nos termos explanados no ponto 39;

f) A reformulação do artigo 5.º por forma a conter a identificação da base legal de suporte às transferências internacionais de dados bem como as salvaguardas adicionais que lhe correspondem;

g) A densificação da obrigação de informação aos titulares dos dados nos termos previstos no Considerando 39 e artigos 13.º e 14.º do RGPD.

h) A previsão da criação de um portal de transparência na plataforma iAP onde os cidadãos possam consultar quais entidades acederam aos seus dados e em que contexto;

i) A alteração do n.º 2 do artigo 7.º por forma a conter uma especificação da informação em causa por tipologias documentais, disposições relativas à granularidade de acesso bem como especificação de limitações de acesso à entidade consumidora;

j) Ainda quando ao artigo 7.º, a previsão no articulado de medidas mitigadoras para o risco de acessos massivos que não cumpram os princípios da minimização de dados;

k) Quanto ao artigo 8.º se consagre a proibição expressa de utilização da plataforma de interoperabilidade para a realização de cópias massivas ou integrais de bases de dados;

l) A reformulação do n.º 3 do artigo 8.º nos termos expostos no ponto 57, bem como a densificação das eventuais exceções decorrentes de alteração do serviço público no n.º 5 deste artigo;

m) Quanto ao artigo 9.º a reformulação do n.º 2 face à contradição com o direito da União Europeia explanado no ponto 62, bem como do n.º 3 deste artigo fixando os procedimentos necessários à efetiva prestação do dever de informação;

n) A previsão no artigo 10.º da necessidade do ato normativo que regula a subcontratação conter a identificação da natureza e finalidade do tratamento por tipologia, a identificação dos tipos de dados pessoais a tratar e ainda as categorias de titulares abrangidos;

o) Ainda quanto ao artigo 10.º a inclusão no n.º 9 da obrigação de notificação dos titulares dos dados;

p) Quanto aos direitos dos titulares que se que se positive no texto em análise a forma de concretização efetiva dos direitos dos titulares;

q) A inclusão de regulamentação sobre canais para pessoas com limitações no acesso digital necessária para garantir o recurso em exclusivo à interoperabilidade através da plataforma de interoperabilidade da administração pública;

r) A previsão de alternativas ao recurso a sistemas ade autorização associados à chave móvel digital no n.º 4 do artigo 14.º do projeto de Decreto-Lei com vista a garantir o princípio da igualdade dos cidadãos;

s) A fixação no n.º 2 do artigo 16-. dos quadros em que os referidos protocolos podem ser realizados, os seus objetos, e qual os elementos obrigatórios que neles tem de constar;

t) A consagração de normas técnicas da plataforma da iAP bem como das medidas de segurança a adotar; e

u) A transposição para o articulado das regras de negócio e imposição de medidas técnicas estabelecidas na AIPD e que não constam do projeto de diploma.

Aprovado na reunião de 19 de maio de 2026

Paula Meira Lourenço (Presidente)

Assinado por: **PAULA CRISTINA MEIRA LOURENÇO**
Data: 2026.05.20 10:39:10+01'00'
Certificado por: **Diário da República**
Atributos certificados: **Presidente - Comissão Nacional de Proteção de Dados**

CARTÃO DE CIDADÃO