PARECER/2026/13

## I. Pedido

1. A Comissão de Assuntos Constitucionais, Direitos, liberdades e Garantias solicitou em 04 de fevereiro de 2026 à Comissão Nacional de Proteção de Dados (CNPD), para se pronunciar sobre o Projeto de Lei 398 XVII 1 (PSD) que *Estabelece medidas de proteção de crianças em ambientes digitais* (doravante Projeto de Lei), cuja discussão na generalidade foi agendada para o Plenário do dia 12 de fevereiro de 2026.

2. O pedido de parecer não veio instruído com qualquer estudo de impacto sobre a proteção de dados pessoais.

3. A CNPD emite parecer no âmbito das suas atribuições e competências enquanto autoridade administrativa independente com poderes de autoridade para controlo dos tratamentos de dados pessoais, conferidos pela alínea c) do n.º 1 do artigo 57º, conjugado com a alínea b) do n.º 3 do artigo 58º e com o n.º 4 do artigo 36º, todos do Regulamento (UE) 2016/679, de 27 de abril de 2016 – Regulamento Geral sobre a Proteção de Dados (doravante RGPD), em conjugação com o disposto no artigo 3º, n.º 2 do artigo 4º e na alínea a) do n.º 1 do artigo 6º, todos da Lei n.º 58/2019, de 8 de agosto, que executa na ordem jurídica interna o RGPD (doravante LERGPD).

## II. Análise

### i. A tutela jurídica dos dados pessoais

4. A Constituição da República portuguesa (CRP) no seu registo normativo sobre os direitos, liberdades e garantias estabelece os direitos fundamentais à reserva da intimidade da vida privada e familiar (artigo 26.º, n.º 1), assim como à autonomia informativa, o que passa pela proteção dos dados pessoais (artigo 35.º, n.º 1 e 2).

5. Trata-se de matéria da competência legislativa exclusiva da Assembleia da República, salvo autorização concedida pela mesma ao Governo, daí designar-se como reserva relativa de competência legislativa (artigo 165.º, n.º 1, alínea *b)* CRP). Quando tal sucede "As leis de autorização legislativa devem definir o objeto, o sentido, a extensão e a duração da autorização, a qual pode ser prorrogada." (artigo 165.º, n.º 2 CRP)

6. Por sua vez, será de referir que a tutela jurídica europeia e nacional específica para a proteção dos dados pessoais a convocar para a apreciação do presente Projeto de Lei, designadamente quanto aos princípios relativos ao tratamento dos dados pessoais, tem o seu núcleo essencial no Tratado sobre o Funcionamento da União Europeia (doravante TFUE), na Carta dos Direitos Fundamentais da União Europeia (doravante CDFUE), e no Regulamento Geral sobre a Proteção de Dados.

7. O TFUE consagra no artigo 16.º, n.º 1 que "[t]odas as pessoas têm direito à proteção de dados de carácter pessoal que lhes digam respeito".

8. Neste alinhamento, a CDFUE estabelece no artigo 8.º que o tratamento dos dados de carácter pessoal deve processar-se no estrito respeito pelos direitos, liberdades e garantias das pessoas singulares, em especial pelo direito à proteção dos dados pessoais (*princípio da legalidade*).

9. A noção legal de dados pessoais está estabelecida no artigo 4.º, 1) do RGPD considerando que os mesmos correspondem à "informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular;".

10. O mesmo RGPD veio consignar no artigo 5.º, n.º 1 que os dados pessoais são: i) Objeto de um tratamento lícito, leal e transparente (*licitude, lealdade e transparência*); ii) Recolhidos para finalidades determinadas, explícitas e legítimas, não podendo ser tratados de forma incompatível com essas finalidades (*limitação das finalidades*); iii) Adequados, pertinentes e limitados ao mínimo necessário à prossecução das finalidades para as quais são tratados (*minimização dos dados*); iv) Exatos e atualizados sempre que necessário, devendo ser tomadas todas as medidas razoáveis para que os dados inexatos sejam apagados ou retificados sem demora (*exatidão dos dados*); v) Conservados de forma a permitir a identificação dos titulares dos dados apenas durante o período necessário para as finalidades para as quais são tratados (*limitação da conservação*); vi) Tratados de uma forma que garanta a sua segurança, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidentais, recorrendo a medidas técnicas ou organizativas adequadas (*integridade e confidencialidade*).

11. Mais será de referir que o RGPD através do artigo 5.º, n.º 2 veio estabelecer o comando de que o responsável pelo tratamento deve adotar as medidas que lhe permitam comprovar que o tratamento de dados pessoais é realizado em conformidade com os princípios enunciados (*responsabilidade*).

12. O *European Data Protection Board* (EDPB) (Comité Europeu para a Proteção de Dados), veio em 11 de fevereiro de 2025, produzir a sua Declaração 1/2025 sobre a certificação da idade, tendo por referência o quadro jurídico europeu, com destaque para o RGPD e o RSD[1].

13. A Comissão Europeia divulgou em 10 de fevereiro de 2026 o designado "Action plan against cyberbulling: Safer online, stronger together" [COM(2026)71], inserindo no mesmo o "Action plan against cyberbulling – protecting children online", referenciando as medidas políticas e legais relevantes para o efeito, destacando no

[1] Acessível em https://www.edpb.europa.eu/our-work-tools/our-documents/statements/statement-12025-age-assurance_pt.

que concerne ao RGPD que os dados pessoais das crianças merecem uma proteção específica e enunciando o seguinte: "O direito ao apagamento dos dados pessoais é particularmente relevante quando o titular dos dados deu o seu consentimento enquanto criança e pode não ter tido plena consciência dos riscos envolvidos, nomeadamente no contexto do ciberbullying"[2].

ii. O Projeto de Lei e a sua sustentabilidade na proteção dos dados pessoais

14. A exposição de motivos encontra-se alicerçada em quatro pilares essenciais: o primeiro vai no sentido de que "[a] ascensão das redes sociais, operada a um ritmo sem precedentes históricos, deslocou silenciosamente funções que durante séculos pertenceram à família, à escola e à comunidade. Essa mudança ocorreu de forma abrupta, sem preparação institucional, sem regulação adequada e sem consciência plena dos custos psicológicos, educativos, sociais e culturais associados".

15. O segundo conjuga "o uso precoce e continuado das redes sociais tem provocado efeitos adversos relevantes na saúde mental e emocional das crianças", com os "prejuízos ao nível da capacidade de concentração, do rendimento escolar e da resistência cognitiva, bem como o isolamento, dificuldades de socialização com colegas, pais, professores e comunidade em geral", incluindo a "exposição a conteúdos inadequados, a vulnerabilidade ao *bullying* e *cyberbullying*, à manipulação emocional, ao aliciamento por terceiros hostis tornou-se uma realidade diária no mundo digital".

16. O terceiro visa estabelecer uma "matriz protetora que a lei estabeleça uma idade mínima clara e adequada para o acesso das crianças aos ambientes digitais, espaço que hoje concentra riscos superiores a outros comportamentos tradicionalmente regulados".

17. O quarto vai no sentido de "estabelecer regras para proteger crianças e jovens, permitindo-lhes navegar com liberdade e segurança no mundo digital e dotando-os de capacidade para tomar decisões informadas sobre as suas atividades online, sem comportamentos aditivos, maximizando os benefícios e minimizando os riscos para o seu bem-estar mental e social"

18. Para o efeito o presente Projeto de Lei contempla vinte e duas (22) disposições, estabelecendo o seu objeto (artigo 1.º), âmbito de aplicação (artigo 2.º), alteração à Lei n.º 58/2019 (LERGPD), definições (artigo 4.º), idade mínima digital (artigo 5.º), consentimento parental (artigo 6.º), obrigação geral de verificação de idade (artigo 7.º), requisitos técnicos da verificação de idade (artigo 8.º), prestadores de conteúdo de risco elevado (artigo 9.º), configurações seguras por defeito (artigo 10.º), prevenção da edição digital (artigo 11.º), proteção contra aliciamento e violência digital sobre as crianças (artigo 12.º), autoridades competentes (artigo 13.º), relatório

[2] Acessível em https://digital-strategy.ec.europa.eu/en/policies/cyberbullying, sendo nossa a tradução.

e transparência (artigo 14.º), contraordenações (artigo 15.º), responsabilidade (artigo 16.º), campanhas públicas de informação (artigo 17.º), certificação de boas práticas (artigo 18.º), avaliação da aplicação (artigo 19.º), cooperação europeia (artigo 20.º), disposição final (artigo 21.º), entrada em vigor (artigo 22.º)

19. O projetado diploma, quer na sua globalidade, quer através de algumas disposições em particular, tem um impacto direto na proteção dos dados pessoais, enquanto outras são susceptíveis de ter um impacto indireto, pelo que iremos apreciar as mesmas.

20. O Projeto de Lei, de acordo com o seu artigo 1º, tem como objeto "estabelecer medidas de proteção de crianças em ambientes digitais", fixando para o efeito, mas agora através do seu artigo 5.º, a idade mínima digital nos 16 (dezasseis) anos (n.º 1), permitindo o acesso relativamente às crianças entre os 13 e os 16 anos de idade, através do consentimento parental informado e expresso (n.º 2), e interditando o acesso aos menores de 10 anos de idade (n.º 3).

21. No entanto, a CNPD verifica que o Projeto de Lei estende o seu âmbito à LERGPD (artigo 3.º), reconfigurando e aumentando a idade mínima de 13 para 16 anos de idade, enquanto critério objetivo, para o consentimento com vista ao tratamento dos dados pessoais.

22. Assim, ocorre uma dessintonia entre o objeto e o âmbito deste Projeto de Lei, que seria aconselhável revisitar.

23. A CNPD também constata que o consentimento digital, enquanto fundamento de licitude de acesso às redes digitais tem carácter objetivo (16 anos de idade), não estabelece quaisquer outros requisitos, designadamente como acontece no consentimento para o tratamento dos dados pessoais (artigo 4.º, 11) do RGPD).

24. Nesta conformidade, sugere-se que as definições constantes no artigo 4.º passem a integrar o "consentimento digital", através da sua densificação através da exigência de uma manifestação de vontade, livre, específica, informada e inequívoca, mediante uma declaração ou ato positivo explícito para aceder às plataformas digitais referenciadas no âmbito de aplicação deste Projeto de Lei (artigo 2.º, n.º 1 e 2).

25. A CNPD também regista a previsão do consentimento parental no que concerne aos menores de 16 anos, que se encontra contemplado nos artigos 5.º, n.º 2 e 6.º do Projeto de Lei, o qual é prestado pelos titulares das responsabilidades parentais.

26. Mas resta saber se a previsão desta exigência legal exige o consentimento de um ou de ambos os progenitores, o que deverá ser esclarecido, sendo de recordar para o efeito o disposto no artigo 1902.º, n.º 1 do Código Civil, onde se preceitua que "se um dos pais praticar acto que integre o exercício das

responsabilidades parentais, presume-se que age de acordo com o outro, salvo quando a lei expressamente exija o consentimento de ambos os progenitores ou se trate de acto de particular importância; a falta de acordo não é oponível a terceiro de boa fé".

27. Mais será de referir que a previsão legal do consentimento parental está essencialmente dirigida para as situações de "normalidade parental" ou então em que a responsabilidade parental está exclusivamente conferida a um dos progenitores, seja pai ou mãe.

28. Porém, as crianças nos casos de divórcio ou de separação dos seus progenitores podem se encontrar numa situação de partilha das responsabilidades parentais, podendo também ocorrer uma situação de institucionalização, em que as responsabilidades parentais podem estar suspensas.

29. Estas situações não se encontram devidamente delineadas no Projeto de Lei e podem ter implicações na tutela dos dados pessoais dos menores de 16 anos de idade, para além de poderem ser uma fonte de conflitualidade parental, em situações pós-conjugais ou pós-união de facto.

30. A CNPD no que concerne à obrigação geral de verificação de idade e aos correspondentes requisitos técnicos, respetivamente previstos nos artigos 7.º e 8.º do Projeto de Lei, considera que se impõe a correspondente análise da robustez técnica do sistema a implementar, em conjugação com a coadunação jurídica decorrente das exigências de proteção dos dados pessoais, nomeadamente na vertente da sua minimização. Este último tratamento de dados pessoais em grande escala, para todas as pessoas maiores de 16 anos de idade, pode não respeitar o teste de proporcionalidade relativamente à proteção dos dados pessoais.

31. Em primeiro lugar, será de questionar se existe um repositório centralizado com a informação sobre a identidade dos titulares das responsabilidades parentais da criança, chamando-se a atenção de que o detentor do exercício da responsabilidade parental pode não ser o respetivo progenitor, sendo atributos completamente distintos.

32. Em segundo lugar, aquando da identificação dos sujeitos que exercem as responsabilidades parentais é necessário igualmente conhecer a identidade da criança. Trata-se de uma condição *sine qua non*, cujo modo de funcionamento não aparenta coadunar-se com a definição avançada na alínea *g)* do artigo 4.º do Projeto de Lei: "comprovar apenas o limiar etário, sem revelar a identidade do utilizador ou outros dados pessoais".

33. Em terceiro lugar, iremos previamente chamar à colação o disposto no n.º 3 do artigo 6º do Projeto de Lei, o qual refere que "as plataformas, serviços, jogos e aplicações acessíveis a crianças devem disponibilizar um painel, acessível à criança e aos titulares das responsabilidades parentais".

34. Ora, a definição funcional estabelecida no referido número mimetiza as funcionalidade existentes nos controlos parentais disponibilizados por detentores de VLOP como o Microsoft Family Safety e o Google Family Link. Estes painéis implicam uma parametrização sobre a informação do agregado familiar e tem de haver um perfil de utilizador, com senha, para que possam ter acesso e preservar as configurações.

35. Nesta conformidade, estamos num cenário em que o operador da plataforma ou serviço digital ficaria com informação sobre o menor e os respetivos responsáveis parentais. Esta implementação não é um mecanismo viável com o pretendido «Sistema de prova de idade com preservação de privacidade».

36. Aliás, no que concerne ao exercício das responsabilidades parentais em ambiente digital, damos conta que na documentação *on-line* Chave Móvel Digital (doravante CMD) está referido que "Não há idade mínima para ter Chave Móvel Digital. Qualquer pessoa adulta, criança ou bebé pode ter uma Chave Móvel Digital, mas precisa de ter o seu próprio número de telemóvel" [3].

37. Com esta premissa, no caso de uso em que a criança não tenha telemóvel, terá de ser um dos titulares da responsabilidade parental a autenticar-se com a sua identidade e garantir a permissão de acesso.

38. A CNPD também considera a necessidade de responsabilização dos titulares das responsabilidades parentais, quando estes sejam autores ou cúmplices de uma utilização ou acesso indevido por parte dos menores a sítios da internet relativamente aos quais deveriam estar excluídos, em virtude de os seus conteúdos não serem ajustados à sua menoridade, como sucede com os designados "conteúdos de risco elevado" Projeto de Lei (artigos 2.º, n.º 1; 9.º, n.º 1).

39. Tal não exclui a responsabilização que deve estar atribuída aos responsáveis pelo tratamento dos dados pessoais e a correspondente verificação da idade mínima para efeitos dos acessos digitais.

40. A CNPD considera que o único modelo preconizado para uso da CMD com vista à validação da faixa etária, que poderia preservar o anonimato do titular dos dados, é o de verificação através da plataforma *autenticaco.gov.pt* e, no passo em que se confronta o utilizador com os atributos que serão transmitidos ao operador cujo serviço ou aplicação implica verificação de idade, apenas deverá surgir o indicador binário, SIM/NÃO, de que o titular é maior de 16 anos. Este indicador, na gíria técnica um "token", transmite ao serviço ou plataforma de destino se o titular dos dados é realmente da faixa etária que permite o seu uso.

41. Não se encontra contemplado na proposta legislativa, mas é importante especificar que o mecanismo de verificação não deve permitir atribuir um identificador nem construir um perfil sobre o respetivo utilizador.

[3] https://www.gov.pt/servicos/ativar-a-chave-movel-digital

42. De igual modo, deve ser desconexo de outros sistemas e impedir a rastreabilidade transversal do utilizador entre diferentes plataformas. Esta é uma prática recorrente nas redes de publicidade digital e de recolha de dados analíticos de utilização.

43. No âmbito da presente proposta e estando em causa pessoas de menoridade, considera-se de todo relevante que o *token* de verificação de idade não seja partilhado de forma alguma. Idealmente, o processo de verificação de idade é totalmente executado na aplicação da carteira/chave móvel digital.

44. A CNPD também sustenta que o *token* em causa deve ter um prazo de validade definido, ao fim do qual será exigida nova verificação.

45. A CNPD no que concerne à proteção contra o aliciamento e violência digital sobre as crianças, constata que o artigo 12.º do Projeto de Lei tem precisamente esse âmbito. No entanto, a responsabilidade é conferida ao serviços e plataformas destinatário do projetado diploma.

46. Porém, a alínea *b)* do n.º 1 do artigo 12.º, pode comportar um nível inadmissível de intrusão pelos agentes económicos na plataformas e serviços digitais que operam. Para conseguir o propósito de bloquear automaticamente mensagens contendo material ofensivo, o operador terá de ter acesso ao conteúdo de todas as mensagens, de todos os utilizadores da plataforma que potencialmente poderão enviar comunicações aos titulares menores de idade. No limite são todos os utilizadores.

47. Tal implica a vigilância e acesso ao teor de todas as comunicações, desvirtuando quaisquer mecanismos de encriptação e inviabilizando comunicações seguras ponto-a-ponto. A pretexto da defesa das crianças, as comunicações e serviços digitais ficam obrigadas a exercer uma vigilância sobre todas as comunicações

48. Nesta conformidade, poderá revelar-se completamente desproporcional, por não ser adequado, necessário e na devida justa medida, realizar o rastreamento e a vigilância do teor de todas as comunicações, podendo ser ainda fonte provável de autocensura. Esta iniciativa, embora preventiva, é intrusiva e deve ser evitada a todo o custo.

49. A CNPD sugere como alternativa viável que, concomitantemente à necessária responsabilização das plataformas e dos prestadores de serviços digitais pelo tratamento dos dados pessoais, haja a implementação de listas de contactos autorizados pelos responsáveis parentais a comunicar com a conta dos menores no serviço ou plataforma digital.

50. A CNPD constata que o artigo 13.º do Projeto de Lei, através do seu n.º 1, atribui à Autoridade Nacional de Comunicações e à Comissão Nacional de Proteção de Dados a competência para "fiscalizar o cumprimento da presente lei, no âmbito das suas competências".

51. Por sua vez, o artigo 15.º do Projeto de Lei vem estabelecer uma lista tipificadora de contraordenações (n.º 1) e das suas sanções (n.º 2), os critérios para a determinação das respetivas coimas (n.º 3), assim como a atribuição de competências para o efeito (n.º 4), nos seguintes termos: "A instrução dos processos de contraordenação compete à Autoridade Nacional de Comunicações ou à Comissão Nacional de Proteção de Dados, no âmbito das respetivas competências, cabendo a decisão à autoridade que tenha instruído o processo".

52. Ora esta regulamentação, essencialmente abstrata e induzivamente incompreensível das competências em razão da matéria para fiscalização e responsabilização contraordenacional, é certamente uma fonte de conflitos negativos ou positivos de competência.

53. Para o efeito, a Proposta de Lei deveria precisar no seu texto o âmbito dessas competências, seguindo, por exemplo, o desenho legislativo da designada Lei das Comunicações Eletrónicas, aprovada pela Lei n.º 41/2004, de 18 de agosto, alterada pela Lei n.º 46/2012, de 29 de agosto, tal como consta no seu artigo 15.º, epigrafado de "Processamento e aplicação de coimas".

54. O Projeto de Lei e retomando o artigo 13.º, mais precisamente o seu n.º 2, dispõe o seguinte: "A Autoridade Nacional de Comunicações, além do regulamento com o Referencial Técnico Nacional de Verificação de Idade previsto no artigo 8.º, pode aprovar outros regulamentos e emitir as orientações técnicas necessárias à plena execução da presente lei, bem como solicitar auditorias independentes aos prestadores de serviços por ela abrangidos."

55. A CNPD constata que este segmento normativo revela fragilidades constitucionais, numa matéria de direitos fundamentais de proteção de dados, que, como anteriormente mencionámos, é da reserva relativa de competência legislativa da Assembleia da República.

56. E isto porque a verificação da idade de acesso às plataformas digitais que estão no âmbito deste Projeto de Lei, exige o tratamento de dados pessoais, tais como o nome e a idade.

57. Deste modo, o designado Referencial Técnico Nacional de Verificação de Idade tem nítidas implicações no domínio da proteção dos dados pessoais, atenta a noção legal conferida pelo RGPD, que o legislador ordinário não pode contornar, atenta a primazia do direito da União Europeia no ordenamento jurídico nacional.

58. Assim, reenviar esta matéria regulamentadora, mais precisamente, os designados "outros regulamentos" para um organismo administrativo, qualquer que seja o mesmo, contende com a exigência constitucional de que a mesma se encontra nos parâmetros de reserva relativa de competência legislativa da Assembleia da República.

### iii. O estudo de impacto da Proposta de Lei na proteção dos dados pessoais

59. A CNPD chama também a atenção para a observância do disposto do artigo 18.º, n.º 4 da Lei n.º 43/2004, de 18 de agosto (Lei de Organização e Funcionamento da Comissão Nacional de Proteção de Dados), segundo o qual "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 pessoais".

60. Deste modo, tal omissão compromete a realização de um parecer sustentado e sustentável quanto à validade e fiabilidade relativamente aos prováveis riscos decorrentes dos tratamentos de dados pessoais constantes nesta Proposta.

## III. Conclusão

61. Nos termos e fundamentos expostos, a CNPD recomenda:

a) A reformulação do objeto do Projeto de Lei de modo a abranger a fixação da idade para o consentimento com vista à proteção dos dados pessoais;

b) A previsão no artigo 4.º do Projeto de Lei da definição do "consentimento digital", estabelecendo a sua densificação;

c) A densificação das previsões em que ocorre o consentimento parental digital, de modo a abranger as situações referenciadas nos itens 25-29;

d) A clarificação do desenho legal da obrigação geral de verificação de idade e do Referencial Técnico Nacional de Verificação de Idade, respetivamente previstos nos artigos 7.º e 8.º do Projeto de Lei, assim como da implementação dos correspondentes mecanismos, atento o referenciado nos itens 30-37;

e) A responsabilização dos titulares das responsabilidades parentais, quando estes sejam autores ou cúmplices de uma utilização ou acesso indevido por parte dos menores a sítios da internet relativamente aos quais deveriam estar excluídos;

f) A implementação de funcionalidades de verificação de idades através do desenho técnico mencionado nos itens 40 a 49;

g) A delimitação e especificação das competências entre a Autoridade Nacional de Comunicações e a Comissão Nacional de Proteção de Dados

h) A eliminação da previsão da implementação de "outros regulamentos" por parte da autoridade administrativa, prevista no artigo 13.º, n.º 2 do Projeto de Lei, ou através de qualquer outra;

i) A realização do respetivo estudo de impacto sobre a proteção de dados pessoais, antes da aprovação do presente Projeto de Lei.

Lisboa, 23 de fevereiro de 2026

Paula Meira Lourenço (Presidente)

Assinado por: **PAULA CRISTINA MEIRA LOURENÇO**
Data: 2026.02.23 23:55:48+00'00'
Certificado por: **Diário da República**
Atributos certificados: **Presidente - Comissão Nacional de Proteção de Dados**

CARTÃO DE CIDADÃO

# Declaração de Voto

1. **Votei favoravelmente o parecer** emitido sobre o Projeto de Lei n.º 398/XVII/1.ª, por concordar, no essencial, com a sua orientação geral quanto à necessidade de reforço da proteção das crianças em ambiente digital e à centralidade das garantias decorrentes do Regulamento Geral sobre a Proteção de Dados.
2. Entendo, contudo, dever explicitar algumas notas complementares de natureza estritamente técnica, atenta a importância desta iniciativa legislativa.
3. **Em primeiro lugar**, o artigo 15.º da proposta cria um regime autónomo de contraordenações que incide sobre deveres diretamente reconduzíveis aos artigos 5.º, 6.º, 8.º, 24.º, 25.º e 32.º do RGPD. Estando tais matérias abrangidas pelo âmbito material do Regulamento, não dispõem os Estados-membros de margem para reconfigurar os limites máximos das coimas. Impõe-se, por conseguinte, a conformação expressa do regime sancionatório ao modelo do artigo 83.º do RGPD, como, aliás, a CNPD já havia salientado na sua **Deliberação 494/2019**, sob pena até de inconstitucionalidade indireta (art.º 8.º, n.º 4 CRP) e violação da primazia do direito da União Europeia.
4. **Em segundo lugar**, a exclusão dos serviços de comunicações eletrónicas interpessoais prevista no artigo 2.º, n.º 3, alínea a), do Projeto de Lei mitiga parte do risco de ingerência nas comunicações privadas. Contudo, em plataformas híbridas - que combinam difusão pública e mensagens privadas internas - a delimitação funcional pode revelar-se insuficiente, sendo necessário clarificar legislativamente se funcionalidades de *messaging* integradas em redes sociais abertas permanecem excluídas. A questão decisiva não é a qualificação formal do serviço, mas a existência ou não de acesso sistemático ao conteúdo das comunicações.
5. O artigo 12.º atribui às plataformas a deteção e limitação de contactos suspeitos e o bloqueamento automático de mensagens contendo material violento ou sexual, incluindo conteúdos agressivos ou falsos que possam configurar cyberbullying.
6. Esta solução pressupõe monitorização sistemática de comunicações privadas, tratamento automatizado de conteúdos e eventual adoção de decisões com efeitos jurídicos ou significativamente análogos para os titulares dos dados (cf. artigos 4.º, n.º 2, 22.º e 25.º do RGPD).
7. Tal solução configura uma transferência funcional de competências materialmente regulatórias para entidades privadas, exigindo densificação normativa clara, critérios

objetivos e mecanismos de fiscalização quanto: aos pressupostos materiais de atuação; aos critérios de qualificação de "contacto suspeito" ou "conteúdo violento"; às garantias procedimentais; aos limites de conservação e reutilização dos dados analisados; aos mecanismos de auditoria e supervisão independente.

8. A ausência de delimitação clara pode implicar tratamentos generalizados de comunicações privadas, potencialmente incompatíveis com os princípios da minimização, necessidade e proporcionalidade (artigos 5.º, 24.º e 25.º do RGPD; artigos 18.º CRP e 52.º CDFUE), bem como com a liberdade de expressão (art.º 37.º CRP).
9. Quanto ao artigo 12.º do Projeto de Lei, importa, pois, sublinhar que o problema central não reside na finalidade de proteção das crianças, mas no carácter potencialmente universal, preventivo e indiferenciado da ingerência nas comunicações privadas. A imposição de bloqueio automático de mensagens pressupõe análise prévia de conteúdo, o que ativa simultaneamente o art.º 5.º da Diretiva 2002/58/CE (cf. "Diretiva ePrivacy" - confidencialidade das comunicações); a Lei n.º 41/2004, de 18.08, alterada pelas Leis n.ºs 46/2012, de 29.08, e 16/2022, de 16.08, bem como os artigos 7.º e 8.º da Carta dos Direitos Fundamentais da União Europeia, o art.º 9.º do Regulamento Geral sobre a Proteção de Dados (se houver categorias especiais), e, eventualmente, o Regulamento (UE) 2021/1232 (derrogação temporária).
10. As comunicações são invioláveis. O art.º 5.º da Diretiva ePrivacy proíbe interceção ou vigilância de comunicações sem base legal específica. Assim, a base jurídica do art.º 12.º do Projeto de Lei não pode ser apenas o art.º 6.º do RGPD.
11. É necessário, antes de mais, ultrapassar a barreira da confidencialidade das comunicações.
12. O Regulamento (UE) 2021/1232 admite, a título excecional e temporário, a deteção voluntária de material de abuso sexual de crianças, sob condições estritas e com derrogação limitada da confidencialidade. O modelo do artigo 12.º, porém, vai além desse quadro excecional, assumindo traços estruturais de generalidade que exigem maior densificação normativa.
13. O problema estrutural do artigo 12.º não reside na finalidade de proteção de menores, mas no carácter potencialmente universal, preventivo e indiferenciado da ingerência nas comunicações privadas, na indeterminação material de conceitos como "conteúdos falsos" ou "agressivos" e na ausência de critérios técnicos objetivos e garantias procedimentais. A sua redação institui um modelo de generalidade que não exige suspeita concreta nem delimitação por risco individualizado, impõe o bloqueio de "mensagens contendo…" (configurando um mecanismo preventivo), utiliza linguagem ampla e elástica - suscetível

de exigir análise semântica e não mero hash/object matching - e estende o dever a comunicações interpessoais (n.º 3), ativando plenamente o regime da Diretiva ePrivacy. Em suma, não estabelece um mecanismo normativo estruturado e delimitado de controlo de comunicações, indo além do Regulamento (UE) 2021/1232, transformando a exceção em regra e invertendo o modelo jurídico europeu.

14. O bloqueio automático de mensagens pressupõe, materialmente, varrimento prévio do conteúdo ou inspeção em trânsito, o que constitui interceção ou vigilância - ainda que algorítmica - subsumível ao artigo 5.º da Diretiva ePrivacy. Tal ingerência não pode assentar apenas no artigo 6.º do RGPD; depende do regime específico da ePrivacy e apenas é admissível nos termos estritos do artigo 15.º dessa Diretiva, isto é, mediante base legal clara, delimitação material, finalidade determinada e respeito pelas exigências de necessidade e proporcionalidade estrita. A base de licitude invocável seria o art.º 6.º, n.º 1, al.ª c) (obrigação jurídica), e, eventualmente, o art.º 9.º, n.º 2, al.ª g), do RGPD. Todavia, aqui entra a jurisprudência do Tribunal de Justiça sobre retenção e vigilância generalizada.
15. O artigo 12.º vai além do quadro específico relativo à deteção de CSAM, incluindo violência, "conteúdos falsos" e cyberbullying, sem moldura europeia equivalente, o que enfraquece a sua defensabilidade à luz da ePrivacy e da Carta.
16. Sem tipificação apertada, mecanismos de recurso e garantias, aumenta o risco de *over-blockin*g (bloqueio de comunicações lícitas) e compressão desproporcionada da liberdade comunicacional.
17. A ausência de densificação aumenta o risco de tratamentos massivos de dados, decisões automatizadas opacas e compressões excessivas da intimidade e liberdade de expressão.
18. Em suma, o art.º 12.º, n.º 1, al. b), e n.º 3, ao impor bloqueio automático de mensagens, pressupõe interceção/vigilância do conteúdo, colidindo com a regra do art.º 5.º da Diretiva ePrivacy e só podendo ser admitido no quadro estrito do art.º 15.º da mesma Diretiva - quadro que a redação atual não satisfaz por generalidade e indeterminação.
19. A obrigação de filtragem/bloqueio automático de comunicações privadas constitui ingerência no sigilo das comunicações (art.º 34.º da CRP) e, pela sua amplitude e conceitos vagos ("falsos", "agressivos"), arrisca também compressão desproporcionada da liberdade comunicacional (art.º 37.º da CRP) e violação das exigências do art.º 18.º da CRP.
20. O simples *scanning* automatizado já constitui ingerência na confidencialidade, tratamento de dados pessoais e potencial perfilagem. A distinção técnica entre interceção penal e análise algorítmica não elimina a ingerência material.

21. Os “Chats” podem revelar uma orientação sexual, religião, saúde, opiniões políticas. Logo, qualquer análise automatizada poderá tratar dados sensíveis (art.º 9.º do RGPD). Nessa hipótese é necessário, à luz do art.º 9.º, n.º 2, do RGPD, base reforçada e garantias acrescidas.
22. A analogia aqui invocada não pretende equiparar estruturalmente os regimes, mas sublinhar a coerência jurisprudencial do Tribunal de Justiça quanto à inadmissibilidade de ingerências generalizadas, preventivas e indiferenciadas sobre comunicações privadas.
23. À luz da jurisprudência consolidada do Tribunal de Justiça sobre retenção e vigilância generalizada (v.g. Digital Rights Ireland, Tele2, La Quadrature du Net, Privacy International), não é admissível uma ingerência universal, preventiva e indiferenciada nas comunicações privadas.
24. Por outro lado, a única base possível em caso de tratamento de dados sensíveis seria a do art.º 9.º, n.º 2, al.ª g) (interesse público importante, com fundamento em lei e com garantias específicas).
25. Há uma diferença estrutural entre um sistema baseado em suspeita concreta, ativado após denúncia, delimitado a contas específicas e com intervenção judicial e o do Projeto de Lei.
26. O Regulamento (UE) 2021/1232 permite, temporariamente, a deteção voluntária de CSAM, sob condições estritas, com relatórios de transparência, e avaliação de impacto. Mas é excecional, é temporário e não autoriza uma vigilância ilimitada.
27. À luz do art.º 34.º da Constituição, só o juiz pode autorizar interceção de comunicações, no processo penal, em casos graves. Se o artigo 12.º permitir análise de conteúdo, fora de processo judicial, por entidades privadas, há um problema constitucional sério.
28. Se o artigo 12.º limitar a deteção a indicadores técnicos específicos, não permitir leitura humana sistemática, for ativado por denúncia ou suspeita, incluir controlo judicial, prever eliminação imediata de dados não relevantes, então a defensabilidade jurídica aumenta substancialmente.
29. Concluindo, importa separar a deteção concreta de controlo estruturado, impedir vigilância universal, limitar tecnicamente a deteção (*hash/object matching*), introduzir garantias procedimentais; observar expressamente a Diretiva ePrivacy, evitar conceitos indeterminados como “conteúdos falsos”.
30. Para não converter a proteção reforçada de menores em serviços digitais e comunicações interpessoais em censura, deve consagrar-se como princípio geral que os prestadores de serviços digitais acessíveis a menores devem adotar medidas proporcionais, necessárias

e adequadas à proteção de crianças e adolescentes contra conteúdos ilícitos ou suscetíveis de causar dano relevante ao seu desenvolvimento.

31. Introduzir-se uma limitação material consistente no facto de as medidas previstas não poderem implicar monitorização generalizada, permanente e indiferenciada do conteúdo das comunicações privadas.
32. Em matéria de deteção concreta de conteúdos ilícitos, os prestadores podem implementar mecanismos automatizados de deteção de:
    a) material que corresponda, por correspondência técnica objetiva, a bases de dados reconhecidas de material de abuso sexual de crianças, nos termos da Diretiva 2011/93/UE e do Código Penal;
    b) outros conteúdos cuja ilicitude resulte de tipificação penal expressa, desde que a deteção assente em critérios técnicos objetivos previamente definidos.
33. Deve estabelecer-se uma proibição de controlo estruturado, ou seja, deve ser vedada a implementação de sistemas de análise semântica generalizada, leitura sistemática ou varrimento contínuo do conteúdo integral das comunicações privadas de todos os utilizadores, salvo nos casos expressamente previstos no direito da União e sujeitos a regime de garantias reforçadas.
34. Em termos de garantias procedimentais, sempre que um conteúdo seja bloqueado ou sinalizado:
    a) o utilizador deve ser informado de forma clara e fundamentada;
    b) deve ser assegurado mecanismo célere de reclamação e reapreciação humana;
    c) o conteúdo não relevante deve ser eliminado sem demora injustificada.
35. Em termos de limitação de finalidade, os mecanismos de deteção previstos:
    a) não podem ser reutilizados para finalidades distintas das previstas na lei;
    b) não podem fundamentar criação de perfis comportamentais ou avaliações generalizadas do utilizador.
36. Em termos de aplicação a serviços de comunicações eletrónicas interpessoais, nos serviços abrangidos pela Diretiva ePrivacy e pela Lei n.º 41/2004:
    a) as medidas devem respeitar o princípio da confidencialidade das comunicações;
    b) apenas são admissíveis ingerências no conteúdo quando expressamente autorizadas por norma da União Europeia ou por lei que cumpra os requisitos do art.º 15.º da Diretiva.

37. Quanto a supervisão e auditoria, os prestadores devem manter registos técnicos das medidas implementadas, sujeitos a auditoria pela autoridade de controlo competente, assegurando transparência, minimização e proporcionalidade.
38. Assim, afigura-se tecnicamente indispensável a densificação normativa do artigo 12.º, mediante delimitação material estrita das situações de intervenção, exclusão expressa de comunicações cifradas ponto-a-ponto, ativação dos mecanismos apenas perante denúncia ou sinal concreto de risco, limitação técnica a critérios objetivos (como *hash matching*), previsão de controlo humano e direito de contestação, e proibição de reutilização dos dados para fins de perfilagem comportamental.
39. **Em terceiro lugar e por último**, não se nos afigura solução tecnicamente equilibrada que, concomitantemente à necessária responsabilização das plataformas e dos prestadores de serviços digitais pelo tratamento dos dados pessoais, haja a implementação de listas de contactos autorizados pelos responsáveis parentais a comunicar com a conta dos menores no serviço ou plataforma digital, com o que divergimos parcialmente do parecer apresentado neste ponto.
40. Na verdade, tal solução pode gerar segmentação relacional excessiva e restrição desproporcionada da autonomia progressiva da criança, deslocando para um modelo rigidamente técnico responsabilidades que devem permanecer, em larga medida, no plano educativo e relacional.
41. O princípio da proporcionalidade (art.º 18.º CRP; art.º 52.º CDFUE) exige que qualquer restrição ao sigilo das comunicações e à liberdade comunicacional seja adequada, necessária e proporcional em sentido estrito. Um modelo assente predominantemente em bloqueio automático e restrição generalizada pode afetar a liberdade de expressão (art.º 37.º CRP; art.º 11.º CDFUE), o direito ao desenvolvimento da personalidade (art.º 26.º CRP) e a autonomia progressiva da criança, não sendo evidente que, na sua configuração atual, supere esse teste.
42. A proteção eficaz das crianças no ambiente digital não se esgota em soluções proibitivas ou de filtragem automática, devendo articular-se com literacia digital, design seguro por defeito, corresponsabilização parental e capacitação progressiva. Deve ponderar-se se modelos exclusivamente assentes em bloqueio satisfazem plenamente o teste de proporcionalidade, à luz da orientação europeia (v.g. Comentário Geral n.º 25 do Comité dos Direitos da Criança), sem prejuízo do recurso a mecanismos já consolidados de controlo parental.

43. **Nestes termos**, acompanho o parecer aprovado, entendendo, todavia, que os aspetos acima referidos merecem clarificação e aperfeiçoamento legislativo, por forma a assegurar plena conformidade com o direito da União Europeia, com os princípios constitucionais da proporcionalidade e da determinabilidade normativa, e com uma proteção efetiva e equilibrada das crianças no ambiente digital.

*José Mário Nogueira da Costa*
Procurador-Geral Adjunto, vogal da CNPD

Assinado por: **JOSÉ MÁRIO NOGUEIRA DA COSTA**
Num. de Identificação: [redacted]
Data: 2026.02.24 14:38:17+00'00'

CARTÃO DE CIDADÃO