



PARECER/2026/31

I. Pedido

1. A Comissão de Assuntos Constitucionais, Direitos, Liberdades e Garantias solicitou em 22 de abril de 2026 à Comissão Nacional de Proteção de Dados (CNPD), para se pronunciar sobre o Projeto de Lei 531/XVII/1ª (CH) correspondente à primeira alteração à Lei n.º 95/2021 que *Regula a utilização e o acesso pelas forças e serviços de segurança e pela Autoridade de Emergência e Proteção Civil a sistemas de videovigilância para captação, gravação e tratamento de imagem e som* (doravante Projeto de Lei), referenciando um prazo indicativo de 10 (dez) dias.
2. A projetada alteração legislativa é dirigida à captação e tratamento de dados biométricos, para efeitos de prevenção de atos terroristas.
3. O pedido de parecer não veio instruído com qualquer estudo de impacto sobre a proteção de dados pessoais.
4. 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 LERGD).

II. Análise

i. A tutela jurídica da vida privada e dos dados pessoais

5. A tutela multinível da vida privada e do tratamento dos dados pessoais projeta-se por distintas plataformas jurídicas, cuja interpretação deve realizar-se de modo harmonioso.
6. Assim, a Declaração Universal dos Direitos Humanos (DUDH), através do seu artigo 12.º consagrou que “[n]inguém sofrerá intromissões arbitrárias na sua vida privada. ...Contra tais intromissões ... toda a pessoa tem direito à proteção da lei”. Por sua vez, o Pacto Internacional dos Direitos Civis e Políticos (PIDCP) seguiu este alinhamento no artigo 17.º, acrescentando a proibição das intervenções ilegais.
7. A nível regional a Convenção Europeia dos Direitos Humanos (CEDH), através do artigo 8.º, precisou o sentido do direito ao respeito pela vida privada (n.º 1), especificando de seguida os requisitos de ingerência da autoridade



pública (n.º 2), a saber: i) a sua consagração mediante a reserva de lei; ii) uma providência necessária numa sociedade democrática; iii), de modo a assegurar qualquer dos interesses aí convencionados, como seja, entre outros, a segurança pública, a defesa da ordem e a prevenção das infrações penais.

8. Por sua vez, a Convenção do Conselho da Europa para a Proteção das Pessoas relativamente ao Tratamento Automatizado dos Dados de Carácter Pessoal, que foi recentemente alterada, passando a designar-se Convenção 108 +, referencia no terceiro considerando do seu Preâmbulo e entre outras coisas a necessidade de garantir a “autonomia pessoal com base no direito de cada pessoa de controlar os seus dados de carácter pessoal e o tratamento de tais dados”.

9. Neste novo alinhamento, expressou no seu artigo 6.º, n.º 1 que “O tratamento de: ... Dados biométricos que identificam uma pessoa de forma única; ... só é permitido se a lei consagrar garantias adicionais às previstas na presente Convenção”, acrescentando no subsequente n.º 2 que “Tais garantias devem proteger contra os riscos que o tratamento de dados sensíveis pode representar para os interesses, direitos e liberdades fundamentais da pessoa em causa, nomeadamente risco de discriminação”.

10. O Tribunal Europeu dos Direitos Humanos (TEDH) tem vindo a considerar que no contexto dos sistemas de uso de tecnologia de reconhecimento facial, através do processamento de dados biométricos, é exigível a «qualidade da lei» (*quality of law*), sendo essencial dispor de regras pormenorizadas reguladoras da aplicação e da determinação do âmbito dessas técnicas de identificação, bem como a existência de garantias sólidas contra o risco de abuso e arbitrariedade, que devem ser mais robustas no que diz respeito à utilização da tecnologia de reconhecimento facial em tempo real (Acórdão Glukhin v. Rússia, de 04/out./2023, proc. 11519/20, §§ 82, 83).

11. A tutela jurídica europeia específica para assegurar os direitos fundamentais à vida privada e à proteção dos dados pessoais a convocar para a apreciação do presente Projeto de Lei, tem o seu núcleo essencial no Tratado sobre o Funcionamento da União Europeia (doravante TFUE) e na Carta dos Direitos Fundamentais da União Europeia (doravante CDFUE).

12. 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”.

13. Por sua vez, a CDFUE diferencia o respeito pela vida privada e familiar (artigo 7.º), da proteção de dados pessoais que lhes digam respeito (artigo 8.º, n.º 1), precisando que estes últimos devem ser objeto de tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei (artigo 8.º, n.º 2).



14. 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).

15. 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)

16. A propósito convém lembrar que o RGPD ao estabelecer a disciplina legal matriz no domínio da tutela jurídica dos dados pessoais, é de aplicação obrigatória e direta, tanto no âmbito da União Europeia, como a nível nacional (artigos 288.º TUE; 8.º, n.º 4 CRP). Para o efeito, passaremos a salientar algumas noções e injunções que têm relevância para a emissão desde parecer.

17. Assim, os dados pessoais 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;” (artigo 4.º, 1) do RGPD).

18. Por sua vez, consideram-se dados biométricos os “dados pessoais resultantes de um tratamento técnico específico relativo às características físicas, fisiológicas ou comportamentais de uma pessoa singular que permitam ou confirmem a identificação única dessa pessoa singular, nomeadamente imagens faciais ou dados dactiloscópicos” (artigo 4.º, 14 do RGPD).

19. 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*).

20. 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*).

21. Por sua vez, o artigo 9.º do RGPD ao disciplinar as categorias especiais de dados pessoais, integra nos mesmos os dados biométricos para identificar uma pessoa de forma inequívoca, cujo tratamento é, em regra, proibido (n.º 1), afastando tal interdição nos casos excepcionais devidamente previstos (n.º 2), como seja por motivos de "interesse público importante", mas sempre sujeito ao teste de proporcionalidade [alínea g)]

22. No que concerne ao âmbito de aplicação material do RGPD, consagra-se no seu artigo 2.º, n.º 2 que "O presente regulamento não se aplica ao tratamento de dados pessoais: d) Efetuado pelas autoridades competentes para efeitos de prevenção, investigação, deteção e repressão de infrações penais ou da execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública."

23. Quando tal sucede, a respetiva disciplina jurídica encontra-se prevista a nível europeu pela Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho de 27 de abril de 2016 e a nível nacional pela Lei n.º 59/2019, de 08 de agosto, que aprovou as regras relativas ao tratamento de dados pessoais para efeitos de prevenção, deteção, investigação ou repressão de infrações penais ou de execução de sanções penais.

24. No entanto, existe uma similitude quanto aos princípios relativos ao tratamento de dados pessoais anteriormente mencionados e previstos no RGPD, com aqueles outros estabelecidos na citada Lei n.º 59/2019 (artigo 4.º, 5.º, 6.º, 7.º e 8.º).

25. Ademais, convém distinguir entre o tratamento de dados biométricos para identificar ou verificar uma pessoa de forma inequívoca, através do método "um para um" (1:1), por um lado, e a identificação biométrica à distância (*remote biometric identification*), mediante o método "um para todos" (1: N), mormente através de interfaces computadorizados e mediante a utilização de inteligência artificial.

26. O Regulamento (UE) 2024/1689 de 13 de junho de 2024, que cria regras harmonizadas em matéria de inteligência artificial, vulgarmente designado por Regulamento de Inteligência Artificial (doravante RIA), veio precisar essa distinção, que teve logo menção no considerando 17 do seu preâmbulo.



27. Assim, começou por estabelecer que o conceito de sistema de identificação biométrica à distância, “deverá ser definido, de modo funcional, como um sistema de IA que se destina à identificação de pessoas singulares sem a sua participação ativa, normalmente à distância, por meio da comparação dos dados biométricos de uma pessoa com os dados biométricos contidos numa base de dados de referência, independentemente da tecnologia, dos processos ou dos tipos de dados biométricos específicos utilizados.”

28. Mais adiante nesse mesmo considerando refere que “Estão excluídos os sistemas de IA concebidos para serem utilizados na verificação biométrica, que inclui a autenticação, cujo único objetivo seja confirmar que uma pessoa singular específica é quem afirma ser e confirmar a identidade de uma pessoa singular com o único objetivo de lhe conceder acesso a um serviço, desbloquear um dispositivo ou ter acesso de segurança a um local”.

29. Nesta conformidade, o artigo 3.º do RIA veio estabelecer as respetivas definições. Assim, considera *dados biométricos*, “os dados pessoais resultantes um tratamento técnico específico relativo às características físicas, fisiológicas ou comportamentais de uma pessoa singular, nomeadamente imagens faciais ou dados dactiloscópicos” (34), enquanto a *identificação biométrica* consiste no “reconhecimento automatizado de características humanas físicas, fisiológicas, comportamentais ou psicológicas para efeitos de determinação da identidade de uma pessoa singular, comparando os dados biométricos dessa pessoa com os dados biométricos de pessoas armazenados numa base de dados” (35). Por sua vez, a *verificação biométrica*, compreende “a verificação automatizada, «um para um», incluindo a autenticação, da identidade de pessoas singulares por meio da comparação dos seus dados biométricos com dados biométricos previamente facultados” (36).

30. Por sua vez, o *sistema identificação biométrica à distância*, corresponde ao “sistema de IA concebido para identificar pessoas singulares, sem a sua participação ativa, normalmente à distância, por meio da comparação dos dados biométricos de uma pessoa com os dados biométricos contidos numa base de dados de referência” (41). Porém, distingue nestes os sistemas em tempo real (42) dos sistemas em diferido (43).

31. Mais será de referir que o RIA, nesse mesmo artigo 3.º, estabelece uma definição de *espaço acessível ao público*, considerando como tal “qualquer espaço físico, público ou privado, acessível a um número indeterminado de pessoas singulares, independentemente da eventual aplicação de condições de acesso específicas e independentemente das eventuais restrições de capacidade” (44).

32. E estas destrições têm particular relevância no domínio das práticas de IA proibidas consagradas no artigo 5.º do RIA, porquanto a admissibilidade de utilização de *sistemas identificação biométrica à distância em tempo*



real, através da sua alínea *h*) do n.º 1, está condicionada aos seguintes pressupostos: *geral*: reserva de lei; *específicos*, sendo estes disjuntivos: *i*) busca seletiva de vítimas específicas de rapto, tráfico de seres humanos ou exploração sexual de seres humanos, bem como a busca por pessoas desaparecidas; *ii*) prevenção de uma ameaça específica, substancial e iminente à vida ou à segurança física de pessoas singulares ou de uma ameaça real e atual ou real e previsível de um ataque terrorista; *iii*) a localização ou identificação de uma pessoa suspeita de ter cometido uma infração penal, para efeitos da realização de uma investigação criminal, ou instauração de ação penal ou execução de uma sanção penal por alguma das infrações referidas no anexo II e puníveis no Estado-Membro em causa com pena ou medida de segurança privativa de liberdade de duração máxima não inferior a quatro anos.

33. Mas estes pressupostos estão condicionados ao requisitos cumulativos do n.º 2 do artigo 5.º do RIA, com vista a confirmar a identidade da pessoa especificamente visada (identificação pessoal específica), tendo em conta os seguintes elementos de ponderação: *a*) a natureza da situação que origina a possível utilização, em especial a gravidade, a probabilidade e a magnitude dos danos causados na ausência da utilização do sistema; *b*) as consequências da utilização do sistema para os direitos e as liberdades de todas as pessoas afetadas, em especial a gravidade, a probabilidade e a magnitude dessas consequências.

34. Mais será de referir, face ao disposto no n.º 3 do artigo 5.º do RIA que “cada utilização de um sistema de identificação biométrica à distância «em tempo real» em espaços acessíveis ao público para efeitos de aplicação da lei, está sujeita a autorização prévia concedida por uma autoridade judiciária, ou uma autoridade administrativa independente cuja decisão seja vinculativa”, salvo as situações de urgência devidamente justificadas, em que se admite a utilização desse sistema sem a correspondente autorização prévia, mas sempre sujeita a uma autorização posterior ratificativa, cuja solicitação deve ser realizada “sem demora injustificada, o mais tardar no prazo de 24 horas”.

35. Por sua vez, o *European Data Protection Board* (EDPB) (Comité Europeu para a Proteção de Dados) e o *European Data Protection Supervisor* (EDPS) (Supervisor Europeu para a Proteção de Dados), apresentaram em 18 de junho de 2021 a sua Declaração Conjunta 5/2021 sobre a proposta do designado Regulamento Europeu do Parlamento e do Conselho sobre as normas harmonizadas em matéria de inteligência artificial¹.

36. A propósito, sustentaram que “[a] identificação biométrica à distância de pessoas em espaços de acesso público implica um risco elevado de violação da privacidade. Por conseguinte, a AEPD e a SEPD consideram que

¹ Acessível em https://www.edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf, sendo nossa a tradução.



é necessária uma abordagem mais rigorosa. A utilização de sistemas de IA poderia suscitar graves problemas de proporcionalidade, uma vez que poderia implicar o tratamento de dados de um número indiscriminado e desproporcional de pessoas para a identificação de apenas algumas (por exemplo, passageiros em aeroportos e estações ferroviárias)” (§ 30 I parte).

37. Acrescentando que “[o] mesmo se aplica aos seus graves efeitos irreversíveis nas expectativas (razoáveis) da população de manter o anonimato nos espaços públicos, o que tem repercussões negativas no exercício da liberdade de expressão, de reunião, de associação e de circulação.” (§ 30 II parte).

38. A EDPB estabeleceu as suas Orientações 05/2022, aprovada em 26 de abril de 2023, sobre a utilização da tecnologia de reconhecimento tecnológico facial no domínio das forças policiais (*on the use of facial recognition technology in the área of law enforcement*)².

39. Nesta enunciou que “[a]s medidas legislativas que servem de base jurídica para o tratamento dos dados pessoais interferem diretamente nos direitos garantidos pelos artigos 7.º e 8.º da Carta. O tratamento de dados biométricos, em todas as circunstâncias, constitui, só por si, uma grave interferência. Tal não depende do resultado, por exemplo, de uma correspondência positiva. Qualquer limitação ao exercício dos direitos e liberdades fundamentais deve ser prevista na lei e respeitar a essência desses direitos e liberdades.”

40. Mais referiu que “[a] base legal deve ser suficientemente clara nos seus termos para dar aos cidadãos uma indicação adequada das condições e circunstâncias em que as autoridades estão habilitadas a recorrer a quaisquer medidas de recolha de dados e de vigilância secreta. Uma mera transposição para o direito interno da cláusula geral prevista no artigo 10.º da LED [*Law Enforcement Directive – Diretiva (UE) 2016/680, de 27 de abril*] careceria de precisão e previsibilidade.”

41. Acrescentou-se ainda que “[a]s medidas legislativas têm de ser adequadas para alcançar os objetivos legítimos da legislação em causa. Um objetivo de interesse geral, por muito fundamental que seja, não pode, por si só, justificar uma restrição a um direito fundamental”.

² Acessível em https://www.edpb.europa.eu/system/files/2023-05/edpb_guidelines_202304_frlawenforcement_v2_en.pdf, sendo nossa a tradução.



42. A CNPD no seu Parecer 2021/143, de 04 de novembro, pronunciou-se sobre a Proposta de Lei n.º 111/XIV/2.^a (GOV) que “Regula a utilização de sistemas de vigilância por câmaras de vídeo pelas forças e serviços de segurança”, o qual está na origem da citada Lei n.º 95/2021³.

43. Nessa Proposta de Lei estava prevista, entre outras situações, “um sistema de gestão analítica dos dados captados”, designadamente de dados biométricos, com a finalidade de prevenção de atos terroristas, mas mediante autorização judicial (cfr. artigos 18.º, n.º 1, 2 e 3).

44. Nesse Parecer 2021/143 considerou-se que “numa Estado de Direito democrático não é admissível a mera previsão de utilização de sistemas de videovigilância em especial com recurso a tecnologias que potenciam os seus efeitos, sem a especificação de condições, limites e critérios necessários a garantir a sua idoneidade para a prossecução de finalidades de interesse público, mas também imprescindíveis para assegurar que a afetação dos direitos fundamentais ocorra na medida do estritamente indispensável e sem excesso” (§ 7).

45. Mais se sustenta que a ausência de um regime legal preciso prejudica a previsibilidade imprescindível num diploma legal, o que “representa um “cheque em branco” à intrusão na vida privada dos cidadãos, como se o facto de se encontrarem em espaços públicos ou de acesso público implicasse a automática negação dessa dimensão humana fundamental. Mais, permitindo ainda, também com grande abertura, *rectius*, com nula densificação normativa, a utilização neste contexto de tecnologias de inteligência artificial, em especial de reconhecimento facial, na aparente ignorância dos riscos de erro e de discriminação que da sua utilização podem resultar” (§ 9)

ii. O Projeto de Lei e a sua sustentabilidade jurídico-legal

46. A exposição de motivos encontra-se alicerçada através de duas constatações, a partir de notícias dos meios de informação: a primeira é que “Portugal tem estado imune a atentados terroristas como os que flagelaram outros Estados europeus, pelo que o grau de ameaça terrorista tem tido um nível que se manteve no moderado (grau 4) até 2023, aquando do ataque do Hamas a Israel, ocasião em que passou a significativo (grau 3) no qual se mantém até agora”; a segunda é que “alguns sinais de aumento do nível de ameaça terrorista mereceram atenção por parte da Europol, que advertiu para um risco mais elevado de situações de terrorismo na União Europeia devido à escalada do conflito do Médio Oriente, que coloca todo o território da UE num nível elevado de ameaça terrorista e de extremismo violento”.

³ O Parecer e a Proposta de Lei estão acessíveis em <https://www.cnpd.pt/comunicacao-publica/noticias/videovigilancia-massiva-e-sem-limites/>.



47. A seguir acantona-se na Estratégia Nacional de Combate ao Terrorismo, aprovada pela Resolução do Conselho de Ministros n.º 40/2023, de 3 de maio, acrescentando que “considera estas linhas de ação dificilmente realizáveis sem recurso à captação e tratamento de dados biométricos”.

48. Para o efeito, o presente Projeto de Lei contempla apenas três (3) disposições, estabelecendo o seu objeto (artigo 1.º - Objeto), acrescentando o n.º 2 ao artigo 16.º da Lei n.º 95/2021 (artigo 2.º - Alteração à Lei n.º 91/2025, de 29 de dezembro) e termina com o dia em que inicia a sua vigência (artigo 3.º - Entrada em vigor) – a epígrafe do artigo 2.º encontra-se indevidamente identificada.

49. O aditamento tem a seguinte redação: “Para efeitos do disposto na alínea e) do n.º 1 do artigo 3.º, é permitida a captação e tratamento de dados biométricos” – este segmento normativo diz respeito à “Prevenção de atos terroristas”.

50. O projetado diploma tem um impacto direto no que concerne ao respeito da vida privada e na proteção dos dados pessoais, muito embora se contenha na prevenção e não se estenda à resposta a atos de terrorismo, mormente através de perseguição a agentes de crimes tipificados como terroristas, através da Lei n.º 52/2003, de 22 de agosto.

51. No entanto, a CNPD constata que o presente Projeto de Lei para além da sua finalidade de prevenção de atos de terrorismo, através da “captação e tratamento de dados biométricos”, corresponde a uma autêntica “norma em branco”, em virtude de não densificar minimamente o respetivo quadro jurídico-legal.

52. Nesta conformidade, revela intensas fragilidades constitucionais numa matéria de direitos fundamentais relativamente ao respeito pela vida privada e à proteção de dados pessoais, que, como anteriormente mencionámos, é da reserva relativa de competência legislativa da Assembleia da República.

53. Mas também não cumpre as exigências de “qualidade de lei”, mormente as estabelecidas pelos regimes legais de proteção de dados e da inteligência artificial, anteriormente assinaladas.

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

54. 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”.



55. 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

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

- a) A reformulação total do Projeto de Lei em consonância com as exigências constitucionais e legais, com vista ao respeito pela vida privada e a proteção dos dados pessoais, precisando o respetivo regime jurídico-legal;
- b) A realização do respetivo estudo de impacto sobre a proteção de dados pessoais, antes da aprovação do correspondente Projeto de Lei.

Aprovado na reunião de 6 de maio de 2026

Paula Meira Lourenço (Presidente)