

PARECER/2026/2

I. Pedido

1. Por despacho do Secretário de Estado da Administração Interna foi solicitado parecer à Comissão Nacional de Proteção de Dados (CNPD) sobre o pedido de autorização de instalação e funcionamento do sistema de videovigilância em Lagos, submetido pela Guarda Nacional Republicana (GNR).
2. O pedido de parecer foi apresentado em 04 de novembro de 2025, nos termos do n.º 3 do artigo 5.º da Lei n.º 95/2021, de 29 de dezembro, que regula a utilização e o acesso pelas forças e serviços de segurança e pela Autoridade Nacional de Emergência e Proteção Civil a sistemas de videovigilância para captação, gravação e tratamento de imagem e som.
3. O pedido vem acompanhado de um documento do qual consta a fundamentação do pedido e a informação técnica do sistema, doravante designado por “Memorando n.º 20/25-GGCG” (doravante Memorando), datado de 03 de novembro de 2025, integrando cinco apensos: Anexo A - Identificação dos pontos de instalação das câmaras; Anexo B - Identificação das características técnicas das câmaras de videovigilância em cada local; Anexo C - Protocolo de cooperação; Anexo D - Avaliação do impacto sobre a proteção de dados; Anexo E – Perfis de acesso ao sistema de videovigilância.

II. Apreciação

i. O quadro jurídico-legal do parecer

4. A Lei n.º 95/2021, de 29 de dezembro (doravante, Lei n.º 95/2021), estabelece através do seu artigo 5.º, n.º 3 que a decisão de autorização é precedida de parecer da CNPD, “que se pronuncia sobre o pedido quanto ao cumprimento das regras referentes à segurança do tratamento dos dados recolhidos e do previsto nos n.º 4 a 6 do artigo 4.º e nos artigos 16.º, 18.º a 20.º e 22.º”
5. Mais se consigna no subsequente n.º 4 do citado artigo 5, que esse parecer é formulado no prazo de 60 dias a contar da data de receção do pedido de autorização, cominando-se na sua parte final que após tal prazo o “parecer é considerado favorável” – tal prazo deve ser aferido em conjugação com a alíneas b) e c) do artigo 87.º do Código do Procedimento Administrativo.
6. Nesta conformidade a pronúncia da CNPD é dirigida a quatro vetores essenciais.
7. O primeiro sobre a conformidade do pedido com as regras referentes à segurança do tratamento dos dados recolhidos.
8. O segundo, diz respeito à proibição de instalação e utilização de câmaras fixas ou portáteis em áreas que, apesar de situadas em locais públicos, sejam, pela sua natureza, destinadas a ser utilizadas em resguardo e ainda a utilização de câmaras de vídeo quando a captação de imagens e de sons abranja os interiores de casa

ou edifícios habitados ou sua dependência ou de estabelecimentos hoteleiros e similares, e quando essa captação afete, de forma direta e imediata, a esfera da reserva da vida íntima e privada.

9. O terceiro, incide sobre a recolha e tratamento subsequente dos dados pessoais, em especial quando realizado através de um sistema de gestão de analítica dos dados captados, por aplicação de critérios técnicos, bem como o respeito pelas condições e limites de conservação das gravações.

10. Por último e em quarto, a CNPD deve verificar se estão assegurados os direitos de informação, acesso e eliminação, com as exceções previstas na lei, relativamente a todas as pessoas que figurem nas gravações obtidas de acordo com a referida lei.

ii. O âmbito e as finalidades da videovigilância

11. No Memorando consta que se pretende instalar vinte e três (23) câmaras em locais públicos do Município de Lagos, mais precisamente das localidades da Praia da Luz, Vila da Luz e seus acessos, Bensafrim, Barão de S. João, Odiáxere e Meia-praia- Palmares, referenciada como sendo áreas sob a jurisdição policial da GNR.

12. Os locais específicos a abranger pelo presente sistema de videovigilância encontram-se identificados na alínea b) e c) do referido Memorando, conforme descrição do Anexo A, correspondendo a estradas municipais, ruas ou avenidas estradais em doze (12) localidades específicas, sendo uma com uma câmara e as demais com duas câmaras.

13. Para o efeito apresenta-se a delimitação da zona geográfica abrangida e estão ilustrados os ângulos/incidências prováveis de visão das câmaras a instalar – descrito no Anexo A.

14. As referidas localizações das 23 (vinte e três) câmaras previstas estão complementadas com a indicação do respetivo ângulo de cobertura de observação em cada local – descrito no Anexo A.

15. No que concerne às características técnicas mínimas gerais é referenciado o seguinte: câmaras IP do tipo Bullet, com sensor único, para instalação no exterior, equipadas com sensor de imagem de 1/1.8" *progressive scan*. Deverão ter ângulos de visualização mínimos de 114º na horizontal e 59º na vertical, controlo dia/noite (visão noturna) e capacidade de introdução de máscaras de privacidade. Adicionalmente, deverão permitir a configuração de regras de análise de vídeo diretamente integradas, com capacidade de deteção de movimentos, tipificação de objetos e geração de eventos, entre outras funcionalidades – cfr. págs. 9 a 17 do Anexo B.

16. São descritas as características e funcionalidade técnicas previstas dos *"servidores de gestão, gravação redundante e software de monitorização"* de suporte ao sistema de videovigilância e do servidor local *"software de gestão e monitorização"* – cfr. págs. 20 a 31 do Anexo B.

17. Também é referido que a monitorização do sistema será assegurada pela Sala de Situação (SSit) do Comando Territorial de Faro (CTer Faro), com a possibilidade de visualização das imagens pelo Centro Integrado Nacional de Gestão Operacional (CINGOp) no Comando Operacional da GNR em Lisboa e ainda com

possibilidade de consultas pela estrutura de investigação criminal, nas instalações do Posto Territorial de Lagos. Estas salas são reservadas e de acesso condicionado apenas a militares da Guarda credenciados para o efeito e com formação para manuseamento do equipamento de visualização das imagens, mediante atribuição de perfis de acesso da Rede Nacional de Segurança Interna (RNSI)

18. Por sua vez, as identificações das características técnicas estão referenciadas na alínea d), ponto 1) do Memorando.

19. Mais será de referir que o equipamento para visualização das imagens será instalado na Sala de Situação (SSit) do Comando Territorial de Faro, localizada no n.º 18 do Largo de S. Sebastião, em Faro, constando ainda na alínea d), ponto 2), que essa zona será “reservada e de acesso condicionado apenas a militares da Guarda credenciados para o efeito e com formação para manuseamento do equipamento”.

20. Acrescentou-se que a transmissão das imagens para a SSit do CTer Faro e para o CINGOp será assegurada através da RNSI, com todas as políticas de segurança nas comunicações que esta rede comporta.

21. Por sua vez, a gravação dos dados registados será efetuada através de um servidor a instalar em compartimento adequado para o efeito no edifício do Posto Territorial de Lagos, sito no Largo do Infantário, Edifício Multifunções S/N - Chinicato - Lagos, ao qual apenas terão acesso os militares da GNR credenciados para tal, sendo esse acesso objeto de registo no sistema à semelhança da SSit do CTer Faro.

22. Menciona-se ainda que o referido equipamento e o sistema de videovigilância:

- a) Permitem unicamente a captação e gravação de imagens, recolhidas quando as pessoas entram no campo de visão do sistema de videovigilância;
- b) Por forma a salvaguardar a recolha de imagens de zonas privadas, as câmaras fazem máscaras privadas diretamente no sensor da câmara e não por *software* ou qualquer outro tipo de encriptação suscetível de descodificação. Essas máscaras são dinamicamente ajustadas, com base no fator de *zoom* atual, e o operador não pode exibir os conteúdos protegidos;
- c) Não procederá a qualquer gravação de som, sem prejuízo da instalação e uso do mecanismo de funcionamento do sistema denominado «*alerta de voz*»;
- d) É referido que o sistema de videovigilância funcionará ininterruptamente durante todo o ano, 24 horas por dia, em todos os dias da semana;
- e) Este sistema de videovigilância possuirá características específicas contra danos e atos de vandalismo e tentativas de intrusão no sistema - descritas no Anexo B;
- f) A responsabilidade pela conservação e tratamento dos dados recairá no Chefe da Secção de Operações, Treino e Relações Públicas do Comando Territorial de Faro, em exercício;

- g) O sistema de videovigilância não permitirá a captação e o tratamento de dados biométricos, inclusive com o recurso às ferramentas de analítica de vídeo e existirão critérios na utilização do sistema de gestão analítica dos dados captados;
- h) Serão garantidos todos os procedimentos de informação ao público sobre a existência do sistema.

23. Recorda-se, todavia, que de acordo com o disposto no n.º 5 do artigo 4.º da Lei n.º 95/2021 as “zonas privadas” correspondem não apenas a edifícios destinados a habitação, mas também estabelecimentos hoteleiros ou similares. Na ausência de especificação, nos elementos fornecidos, da finalidade de utilização dos edifícios captados nas imagens, a CNPD recomenda que a colocação das máscaras seja também assegurada em eventuais estabelecimentos hoteleiros ou similares, sob pena de violação do n.º 5 do artigo 4.º da Lei n.º 95/2021.

iii) Avaliação técnico-jurídica

24. Na AIPD e na descrição das “Medidas de mitigação previstas para fazer face aos riscos”, menciona-se, entre outras coisas, que:

- a. *«a entrada nas salas onde é possível a visualização de imagens é assegurada apenas aos militares credenciados para o efeito, mediante a introdução de um código de entrada ou leitura de impressão digital»*. Era conveniente clarificar qual o método que vai ser instalado/usado e, caso o acesso à sala for por código, cada militar deve ter um código diferente para que seja possível determinar quem se encontrava no espaço num dado momento temporal – pág. 9, “*Segurança do tratamento de dados, al. a)*”;
- b. o acesso ao servidor onde os dados estarão guardados (Quartel da GNR de Lagos) realiza-se através da introdução de um código de entrada. Será conveniente clarificar se este código de entrada é de acesso ao servidor ou à sala onde irá estar localizado – pág. 10, “*Segurança do tratamento de dados, al. d)*”;
- c. a possibilidade de existir *«o subcontratante»*, mas não se identifica qual nem o contexto/âmbito da prestação de serviços – pág. 10, “*Segurança do tratamento de dados, al. e)*”. Se este subcontratante intervir na manutenção/assistência, esta não pode ser remota;
- d. *«O Software instalado possui proteção contra cyber-ataques»*, mas não se menciona que tipo de proteção está em causa e para quais tipos de ataque – pág. 10, “*Segurança do tratamento de dados, al. f)*”;
- e. *«As câmaras aceitam cartões SD para registar vídeos no seu interior em caso de quebra de rede...»*. Porém, não é claro quais os procedimentos de uso e segurança no transporte dos mesmos – pág. 11, “*Segurança do tratamento de dados, al. i)*”;

f. «Por forma a salvaguardar a recolha de imagens de zonas privadas, as câmaras fazem máscaras privadas diretamente no sensor da câmara e não por software ou qualquer outro tipo de encriptação suscetível de descodificação». Contudo:

- (i) As câmaras n.º 1, 2, 4, 5, 9, 10, 12, 13, 15, 20, 22 e 23, tendo em consideração as fotografias apresentadas nas figuras 2, 5, 9, 11, 19, 21, 25, 26, 30, 40, 45 e 47, respetivamente, não apresentam qualquer máscara privada e, atendendo às características técnicas dos equipamentos, têm potencial para captar imagens do interior de zonas privadas, habitações ou respetivas dependências;
- (ii) As câmaras n.º 3, 6, 7, 8, 11, 17, 18 e 19, considerando as fotografias apresentadas nas figuras 7, 13, 15, 17, 23, 35, 37 e 39, respetivamente, embora possuam máscaras privadas sobre algumas áreas, continuam, em função das suas características técnicas, a apresentar possibilidade de captação de imagens do interior de zonas privadas, habitações ou dependências;
- (iii) As câmaras n.º 14, 16 e 21, conforme as fotografias apresentadas nas figuras 29, 32 e 43, respetivamente, não têm atualmente no seu campo de visão qualquer zona privada, habitações ou dependências. No entanto, deverá ser prevista a aplicação de máscaras sempre que a morfologia da área sofra alterações que possam expor tais zonas.

25. A CNPD, na sequência das disposições legais anteriormente mencionadas, relembra que a privacidade não tem de ser salvaguardada apenas dentro dos edifícios, mas também no acesso aos mesmos, máxime quando se trate de edifícios destinados a habitação (por a informação sobre com quem se entra na própria casa, ou quem aí é recebido, ser, diretamente, informação relativa à vida privada e que merece reserva).

26. Demais, alerta-se para o facto de as máscaras de privacidade terem de ser configuradas em termos que garantam que os operadores não as possam remover, sendo essencial que sejam adotadas medidas efetivas garantias de privacidade, quer no momento da sua definição (pelo instalador), quer quanto ao tipo de credencial necessária para a sua desativação.

27. A CNPD considera não ser claro que o “objeto” a visualizar e a gerar eventos sejam unicamente “humanos” e respetivos movimentos, porquanto constam referências a veículos (motorizados e não motorizados), vagas de estacionamento, estatísticas de tráfego, reconhecimento de matrículas (em tempo-real), pesquisa de registos de veículos, entre outras menções não relacionadas com “humanos” – doc. Anexo B.

28. Mais será de referir, igualmente e no que respeita ao objeto “humano”, existir a indicação de “Captura de rosto em tempo real pela câmara” e também a menção a exibir “informações sobre humanos”, entre outras referências relacionadas – doc. Anexo B.

29. Por outro lado, existem duas instalações distintas para “monitorização do sistema”, sendo uma na Sala de Situação (SSit) do Comando Territorial de Faro (CTer Faro), estando a outra no Centro Integrado Nacional de Gestão Operacional (CINGOp) no Comando Operacional da GNR em Lisboa – pág. 7, Anexo D.

30. Mais será de referir no que concerne à arquitetura de comunicações e de transmissão de imagens, que a «transmissão das imagens para a SSit do CTer Faro será assegurada» pela Rede Nacional de Segurança Interna (RNSI) com «com todas as políticas de segurança nas comunicações que esta rede comporta (Protocolos seguros de comunicação (TLS/SSL))».

31. Nesta conformidade, a CNPD considera-se que devia ser clarificado quais as políticas de segurança em causa para o sistema de videovigilância em análise. Esta questão da RNSI já foi detalhada e exposta na INFORMAÇÃO/2021/70 apensa ao processo PAR/2021/80 relativo a Albufeira e no PARECER/2025/37 apensa ao processo PAR/2024/72 relativo a Vilamoura.

32. Ainda sobre características técnicas:

- a. É recomendável que os protocolos que não estão a ser usados sejam desativados nas câmaras (ex: HTTP, RTSP, SSH, ONVIF, etc.);
- b. Se a transmissão das imagens realiza-se através da rede é digital, o protocolo deve ser cifrado com TLS1.2 ou superior e/ou com um *Codec* proprietário do fabricante.

33. Acerca de perfis de utilizadores, considera-se que deve ser clarificado se os perfis de acesso à sala e de acesso ao sistema de videovigilância são os perfis do próprio sistema e equipamentos descritos no Anexo B ou se são os «*perfis de acesso RNSI*» atribuídos ou a atribuir.

34. Ainda acerca de perfis de acesso, de acordo com o mencionado Anexo E, existirão:

- a. *Perfil de Operador*, atribuído a militar da GNR que se encontre na sala de situação do CTer Faro, permite:
 - (i) Visualização das imagens gravadas e em tempo real, com possibilidade de destacar e fixar determinada câmara, sempre que exista necessidade de monitorizar determinada ocorrência em tempo real;
 - (ii) Ainda a busca por características de identificação do objeto, nos casos devidamente fundamentados e expressos na legislação vigente e no documento anexado, mas não permite a criação ou ativação de qualquer regra de analítica de vídeo, bem como a extração de imagens.
- b. *Perfil de Consulta*, atribuído ao Oficial/Graduado de Serviço da Sala de Situação, que possui responsabilidades de supervisão e monitorização de toda atividade operacional da Unidade, permite a criação ou ativação de regras de pesquisa com recurso as ferramentas de analítica de vídeo

disponibilizadas pelo sistema, por forma a assegurar resposta a ocorrências que surjam em tempo real, e que impliquem tomada de decisões imediatas em resposta a incidentes que configurem crime ou áreas de proteção civil que coloquem em risco o bem jurídico “vida”. Este perfil permitirá também aos militares afetos à atividade de investigação criminal a criação ou ativação de regras de pesquisa com recurso às ferramentas de analítica de vídeo, sempre que exista interesse ao nível da investigação criminal ou que seja solicitado pelas autoridades judiciais.

- c. *Perfil técnico*, para além de todas as permissões dos perfis anteriores, possibilita realizar a extração de imagens e alterar as configurações técnicas dos equipamentos, mediante prévia validação do Chefe da Secção de Operações Treino e Relações Públicas.
- d. *Perfil de Administrador*, atribuído ao responsável pela conservação e tratamento dos dados, Chefe da Secção de Operações, Treino e Relações Públicas, em exercício – permite:
 - (i) Gestão integral do sistema;
 - (ii) Supervisiona e autoriza a extração de imagens decorrentes dos processos judiciais;
 - (iii) Autorização da aplicação da analítica de dados.

35. A CNPD deve pronunciar-se sobre o respeito pelo artigo 16.º da Lei n.º 95/2021, nos termos do n.º 3 do artigo 5.º da mesma lei.

36. Ora, os critérios de analítica dos dados captados – que o legislador nacional denominou de «técnicos» – têm significativa relevância na avaliação da proporcionalidade desta específica operação de tratamento de dados pessoais, por serem suscetíveis de impactar sobre direitos, liberdades e garantias dos cidadãos.

37. Para o efeito, é exigível que seja objeto de uma ponderação específica sobre a sua adequação e necessidade face aos fins especificamente visados com a sua utilização, por parte de quem os define (o responsável pelo tratamento), bem como pelo órgão que, em sede de procedimento autorizativo, exerce a competência autorizativa do tratamento, bem como pelo órgão com explícita competência consultiva nesta matéria (a CNPD).

38. Cabendo à CNPD emitir parecer sobre a aplicação concreta da tecnologia prevista no artigo 16.º da Lei n.º 95/2021, nos termos do n.º 3 do artigo 5.º do mesmo diploma, pronúncia que é essencial para que o membro de Governo com competência autorizativa possa avaliar da proporcionalidade do tratamento de dados pessoais decorrente da utilização do sistema de videovigilância e, portanto, também desta específica operação de tratamento, de acordo com o disposto nos n.ºs 1 a 3 do artigo 4.º da Lei n.º 95/2021, seria, para o efeito, indispensável a identificação e explicação (fundamentação) dos critérios que vão orientar a aplicação das funcionalidades anteriormente descritas.

39. Por outro lado, não basta afirmar que o sistema não permite que haja tratamento de dados biométricos, sem se justificar essa conclusão, porquanto pode haver eventualmente a capacidade de reconhecimento facial, pela simples razão de que existe captação de imagens humanas.

40. Por outras palavras, as salvaguardas de natureza meramente declarativa ou intencional, são manifestamente insuficientes para assegurar que a operação de analítica dos dados não implique a discriminação em função de fatores constitucional e legalmente proibidos, nada havendo na descrição do sistema de gestão que demonstre estar afastado tal risco.

41. Em suma, é indispensável a apresentação dos critérios de análise dos dados, sob pena de não se poder avaliar se este tratamento respeita os diferentes limites e condições previstos na lei e na Constituição da República Portuguesa. E é ainda essencial que se preveja que o código fonte, que se vai utilizar neste sistema, seja auditável, sob pena de se esvaziar a função e os poderes de fiscalização legalmente atribuídos à CNPD.

42. Deste modo, face à omissão, no pedido, na Fundamentação e na AIPD, da identificação dos critérios subjacentes à utilização do sistema de gestão de analítica de dados, a CNPD não consegue verificar se são respeitadas as condições e os limites constitucionais ou legais para essa utilização, nem o órgão com competência autorizativa tem elementos suficientes para avaliar a proporcionalidade da mesma.

43. Mais acresce, conforme anteriormente foi mencionado no ponto 24, com referência ao descrito na alínea f), existem diversas câmaras de videovigilância com manifesto potencial para captar imagens do interior de zonas privadas, habitações ou respetivas dependências ou então de atividades hoteleiras ou similares.

III. Conclusão

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

- a. A delimitação das finalidades de proteção das pessoas, animais e bens e de prevenção e repressão criminais, por um lado, e de gestão rodoviária e prevenção e repressão de infrações estradais, por outro, pelos diferentes conjuntos de câmaras de videovigilância, em função dos riscos por área ou zona, de modo a permitir a avaliação da proporcionalidade do sistema de videovigilância, assim como da proporcionalidade do pretendido sistema de gestão analítica das imagens;
- b. As máscaras de ofuscação para garantia da privacidade devem ser efetivamente aplicadas em todas as janelas e portas dos edifícios destinados a habitação e a atividades hoteleiras ou similares, e devem estar configuradas conforme indicado supra, no ponto 24, alínea f);
- c. A adoção de medidas capazes de garantir a segurança do sistema e a auditabilidade do tratamento de dados pessoais;
- d. A imprescindibilidade de ficar expressa e claramente delimitada a existência de eventuais sub-subcontratantes.



45. A CNPD recomenda a não autorização da utilização do proposto sistema de gestão de analítica de dados, em face da ostensiva ausência (no pedido e nos elementos que o instruem, máxime na avaliação de impacto sobre a proteção de dados) de definição dos respetivos critérios subjacentes, pela impossibilidade de verificação do respeito pelas condições e limites legais e constitucionais à sua utilização, bem como de avaliação da proporcionalidade dessa utilização.

Aprovado na reunião de 6 de janeiro de 2026

Paula Meira Lourenço (Presidente)

Assinado por: **PAULA CRISTINA MEIRA LOURENÇO**
Data: 2026.01.06 20:02:17+00'00'
Certificado por: **Diário da República**
Atributos certificados: **Presidente - Comissão Nacional de Proteção de Dados**

