CNPD
Comissão Nacional de Proteção de Dados

PARECER/2025/38

I. Pedido

1. O Secretário de Estado da Administração Interna solicitou parecer à Comissão Nacional de Proteção de Dados (CNPD) sobre o pedido de autorização de instalação e funcionamento de um sistema de videovigilância no Palácio Nacional de Mafra, que lhe foi submetido pela Guarda Nacional Republicana (doravante GNR).

2. O pedido foi apresentado, nos termos do n.º 3 do artigo 5º da Lei n.º 95/2021, de 29 de dezembro, (doravante Lei n.º 95/2021), que regula a utilização e 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. Em 29 de novembro de 2021 foi celebrado entre a GNR e a Câmara Municipal de Mafra um protocolo para implementação de um sistema de videovigilância em locais públicos, constituído por 4 câmaras, abrangendo as imediações do Palácio Nacional de Mafra, do Terreiro D. João V, do Largo do Conde de S. Januário, da Praça da República e nos acessos rodoviários e pedonais a essas áreas.

4. O pedido vem acompanhado de 5 anexos:

- Anexo A – Identificação dos locais de instalação das câmaras;
- Anexo B – Identificação das características técnicas das câmaras a instalar em cada local;
- Anexo C – Protocolo de cooperação;
- Anexo D – Avaliação de Impacto sobre a proteção de dados;
- Anexo E- Perfis de acesso ao sistema de videovigilância.

II. Objeto do parecer a emitir nos termos da Lei n.º 95/2021, de 29 de dezembro

5. A CNPD aprecia o pedido nos termos e para os efeitos do número 3 do artigo 5.º da Lei n.º 95/2021, de 29 de dezembro (doravante Lei n.º 95/2021), 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, em conjugação com as alíneas b) e c) do artigo 87º do Código de Procedimento Administrativo.

6. Nos termos dessa norma legal, o âmbito do parecer a emitir pela CNPD circunscreve-se à matéria do cumprimento das regras de segurança do tratamento de dados recolhidos, bem como à recolha e tratamento de dados (artigo 16.º), aos aspetos procedimentais no caso de registo da prática de factos com relevância

criminal (artigo 18.º), aspetos relativos à conservação das gravações (artigo 19.º), com direitos do titular de dados (artigo 20.º) e com as condições de instalação (artigo 22.º).

7. Nessa conformidade, deve a CNPD verificar se estão asseguradas, a todas as pessoas que figurem em gravações obtidas pelo sistema, as condições para o exercício dos direitos de acesso e eliminação, quando aplicáveis e garantido o direito de informação, bem como apreciar e pronunciar-se sobre a recolha e processamento dos dados pessoais, em especial se realizado através de gestão analítica dos dados captados, por aplicação de critérios técnicos.

III. Videovigilância em locais públicos de utilização comum

A – Descrição:

8. O pedido de Parecer reporta-se à instalação de um sistema de videovigilância constituído por 4 câmaras fixas, colocadas na Rotunda EN 116 – Largo General Humberto Delgado; Claustro Norte; Claustro Sul e Rotunda de acesso à Escola de Aramas.

9. No Anexo A está delimitada a zona geográfica abrangida e assinalados os ângulos/incidências de visão das câmaras a instalar.

10. As câmaras a instalar são câmaras com multisensores de imagem e função PTZ-PAN (movimento panorâmico); TLT (movimento vertical) e Zoom (movimento de apreciação ou distanciamento), com cobertura de visualização de 360.º

11. Todos os equipamentos capturam imagens em permanência, por disporem de visão noturna, têm capacidade para introdução de máscaras de privacidade, de configuração de regras de análise de vídeo com capacidade de deteção de movimentos, tipificação de objetos e geração de eventos, (Anexo B, pág. 6 a 12).

12. O sistema de monitorização será instalado na Sala de Situação (SSit) do Comando Territorial da Lisboa (Cter Lisboa), sala reservada e de acesso condicionado, apenas permitido a militares da GNR credenciados para o efeito, mediante atribuição de perfis de acesso da Rede Nacional de Segurança Interna (doravante RNSI).

13. A transmissão das imagens para a "SSit do Cter de Lisboa" será assegurada através da RNSI com todas as políticas de segurança nas comunicações que esta rede comporta.

14. 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 Mafra, ao qual apenas terão acesso os militares da GNR credenciados para tal, sendo o acesso objeto de registo no sistema tal como ocorre com o acesso à sala de SSit.

15. O equipamento de videovigilância:

a) Apenas procederá à captação e gravação de imagens quando as pessoas entrarem no campo de visão do sistema de videovigilância;

b) Para salvaguarda da privacidade as câmaras introduzem máscaras diretamente no sensor da câmara e não através de software ou qualquer outro tipo de encriptação, suscetível de descodificação. Tais máscaras são dinamicamente ajustadas através do uso do Zoom, não permitindo que o operador possa exibir os conteúdos protegidos;

c) Não procederá a gravação de som, sem prejuízo da instalação e uso do sistema denominado "alerta de voz";

d) Possui proteção contra danos, atos de vandalismo e tentativas de intrusão no sistema;

e) O responsável pela conservação e tratamento dos dados é o Chefe de Secção de Operações, Treino e Relações Públicas do Comando Territorial de Lisboa, em exercício;

f) Serão garantidos todos os procedimentos de informação ao público sobre a existência do sistema.

g) No Anexo E é feito constar que a plataforma permite a criação de três perfis de utilizadores: *Perfil de Operador* (atribuído a militar da GNR que se encontra na Sala de Situação do CTer em Lisboa) e permite a visualização das imagens em tempo real, com possibilidade de destacar e fixar determinada câmara, sempre que exista necessidade de monitorizar uma ocorrência em tempo real, assim como, com prévia autorização do Oficial/Graduado de Serviço da Sala de Situação, permite a extração de imagens e a consulta ou ativação de qualquer regra de analítica de vídeo; *Perfil de Consulta*, (atribuído ao Oficial Graduado de Serviço da Sala de Situação em exercício e aos elementos do Núcleo de Investigação Criminal de Mafra) que permite: visualizar as imagens em tempo real; consultar ou dar permissão para que sejam consultadas as imagens gravadas; criar ou dar permissão para a criação de regras de pesquisa com recurso às ferramentas de analítica de vídeo disponibilizado pelo sistema - consultas que são alvo de registo em formulário próprio e validadas posteriormente pelo responsável pela conservação e tratamento dos dados – Chefe da Secção de Operações, Treino e Relações Públicas em exercício; permite o acesso a imagens gravadas e pesquisa com recurso às ferramentas de analítica de vídeo, sendo a extração sempre validada pelo responsável pela conservação e tratamento dos dados, Chefe da Secção de Operações, Treino e Relações Públicas em exercício; *Perfil de Administrador*, que é atribuído ao responsável pela conservação e tratamento dos dados, Chefe de Secção de Operações, Treino e Relações Públicas em exercício e permite: A gestão integral do sistema, a supervisão e a

autorização da extração de imagens para processos judiciais e autoriza o uso da aplicação da analítica de dados.

B – Análise:

16. Quanto à segurança física do sistema:

a) Na AIPD, no que se refere às medidas de mitigação dos riscos, é referido que o controlo de entrada nas salas de visualização de imagens é feito através de código de entrada ou leitura de impressão digital. Importa que seja clarificado o meio que será implementado e, caso se opte por acesso por meio de código, a cada militar deve ser atribuído um código individual para permitir a identificação de quem esteve na sala num determinado momento.

b) Sendo o acesso ao servidor em que os dados estão guardados feito através de código de entrada, mostra-se necessário esclarecer se esse código de entrada se refere ao acesso direto ao servidor ou se se refere ao acesso à sala em que este se encontra localizado.

c) No capítulo sobre "Segurança no tratamento de dados", (página 9 da AIPD) é feita referência a "subcontratante", mas não é identificada a entidade, nem o âmbito desses serviços. No caso do subcontratante intervir na manutenção ou prestação de assistência deve ser garantido que assa assistência não seja realizada remotamente.

d) É referido, relativamente à segurança do tratamento de dados (Pág. 9, alínea f), que o "software instalado possui proteção contra cyber-ataques". Contudo, não é indicado o tipo de proteção adotado e para que tipo de ataques, o que não permite que a CNPD se pronuncie sobre a eficiência do mesmo.

e) É ainda referido que "as câmaras aceitam cartões SD para registar vídeos no seu interior em caso de quebra de rede", mas essa informação é insuficiente. Deverão ser especificados os procedimentos de manuseamento, armazenamento e segurança no transporte dos mesmos.

17. Quanto aos mecanismos de auditoria e utilização do sistema:

f) Deverá ser definida uma política de retenção dos registos de atividade, fixando prazo para retenção dos dados e indicadores-chave para os relatórios de auditoria em sede de monitorização da segurança nos acessos e das operações efetuadas. É expectável que esses registos, que devem conter dados das operações realizadas e não dados pessoais, tenham um prazo de conservação adequado para permitir a deteção de padrões ou a reconstrução de acessos e ações anómalas, sob pena da sua finalidade ficar esvaziada, pelo que, à semelhança de outras situações, a CNPD recomenda a conservação dos registos de auditoria pelo prazo de dois anos.

18. Quanto à arquitetura de comunicações e de transmissão de imagens:

g) É referido que na comunicação e transmissão de imagens será usada a RNSI, a qual assegura "todas as políticas de segurança". Mostra-se necessário proceder à clarificação das políticas de segurança aplicáveis especificamente ao sistema de videovigilância de molde a garantir total transparência relativamente aos protocolos de proteção, encriptação e controlo de acessos implementados.

19. Quanto às caraterísticas técnicas:

h) É indicado que as câmaras contêm um servidor da Web integrado para captura de vídeo e configuração disponível num navegador de internet padrão, usando o protocolo HTTP sem necessidade de software adicional. O protocolo HTTP não é cifrado, pelo que esta funcionalidade apresenta uma vulnerabilidade de acesso em caso de comprometimento da rede, pois pode existir captura de credenciais de acesso às câmaras. Importa trocar a senha que vem de fábrica para evitar que o sistema fique comprometido desde o início. Importa, igualmente, reconfigurar o servidor integrado para HTTPS e implementar uma política de gestão das senhas nas câmaras, afastando a utilização de uma senha única para todos os equipamentos.

i) É indicado que as câmaras são compatíveis, entre outros, com os protocolos IPv4; IPv6, HTTP, HTTPS, DNS, NTP, RTSP, RTCP, RTP, TCP, UDP, IGMP, ICMP, DHCP e ARP. Todos os protocolos não essenciais para o funcionamento do sistema deverão ser desativados por razões de segurança.

j) Sendo utilizada a rede digital para transmissão das imagens, recomenda-se que o protocolo utilizado seja cifrado, usando a encriptação TLS (Transport Layer Security) 1.2, ou superior (porquanto apenas a versão TLS 1.2, ou superior, dá garantias de segurança nas comunicações) e/ou utilize um Codec do fabricante.

20. Quanto à autenticação e perfis dos utilizadores - art.º 3.º da Portaria n.º 372/2012, de 16 de novembro:

k) Na documentação apresentada é afirmado que a visualização das imagens é feita exclusivamente por militares credenciados para o efeito, mediante a introdução de um código de entrada ou leitura de impressão digital. Deve assegurar-se que se o mecanismo escolhido for o código, este é pessoal e intransmissível.

l) Entende-se que a extração de imagens deve ser uma funcionalidade de acesso privilegiado e deverá existir registo de quais as câmaras acedidas, intervalo temporal na extração, bem como identificação do responsável pela execução.

21. Sobre os procedimentos de extração de imagem:

No Anexo D, que contém a AIPD, está previsto que «o acesso aos dados e a respetiva extração de gravações das imagens vídeo dependerá de despacho prévio de autorização pelo responsável pelo tratamento de dados (…)» e ainda que «as gravações definidas pelo Ministério Público com interesse para a investigação criminal serão guardadas até ao final do processo-crime». Nada mais é referido sobre a extração de imagens, designadamente sobre como são preservadas estas gravações para serem excluídas do prazo de 30 dias do arquivo do sistema.

22. No que se refere à recolha de imagens, deve ser contemplado na solução que o software de gestão do sistema de videovigilância tem mecanismos que viabilizam a exportação em formato digital, assinado digitalmente, que ateste a veracidade do seu conteúdo. Deverá, igualmente, aludir-se à presença de mecanismos de cifra caso se pretenda proteger a exportação com uma senha de acesso ou outro fator de segurança.

Conclusões

23. A CNPD, ao abrigo da competência que lhe é conferida pela Lei n.º 95/2021 e nos termos e fundamentos expostos supra expostos, recomenda:

a) Que seja clarificado o meio a implementar para o controlo de entrada nas salas de visualização de imagens e, caso se opte por acesso por meio de código, a cada militar deve ser atribuído um código individual para permitir a identificação de quem esteve na sala num determinado momento;

b) Sendo o acesso ao servidor em que os dados estão guardados feito através de código de entrada, mostra-se necessário esclarecer se esse código de entrada se refere ao acesso direto ao servidor ou se se refere ao acesso à sala em que este se encontra localizado;

c) No capítulo sobre "Segurança no tratamento de dados", (página 9 da AIPD) é feita referência a "subcontratante", mas não é identificada a entidade, nem o âmbito desses serviços. No caso do subcontratante intervir na manutenção ou prestação de assistência deve ser garantido que essa assistência não seja realizada remotamente;

d) Deve ser esclarecido que tipo de proteção contra cyber-ataques possui o software instalado e para que tipo de ataques;

e) Relativamente aos cartões SD para registar vídeos no seu interior em caso de quebra de rede", importa que sejam especificados os procedimentos de manuseamento, armazenamento e segurança no transporte dos mesmos;

f) Seja definida uma política de retenção dos registos de atividade, fixando prazo para retenção dos dados e indicadores-chave para os relatórios de auditoria em sede de monitorização da segurança nos acessos e das operações efetuadas.

Lisboa, 3 de junho de 2025

Paula Meira Lourenço (Presidente)

Assinado por: **PAULA CRISTINA MEIRA LOURENÇO**
Data: 2025.06.03 21:35:00+01'00'
Certificado por: **Diário da República**
Atributos certificados: **Presidente - Comissão Nacional de Proteção de Dados**

CARTÃO DE CIDADÃO