CNPD
Comissão Nacional
de Proteção de Dados

# PARECER/2021/93

## I. Pedido

1. Por despacho do Secretário de Estado Adjunto e da Administração Interna, foi solicitado parecer à Comissão Nacional de Proteção de Dados (CNPD) sobre o pedido de autorização de instalação e um sistema de videovigilância na cidade de Santarém, submetido pela Polícia de Segurança Pública (PSP).

2. A CNPD aprecia o pedido nos termos do n.º 2 do artigo 3.º da Lei n.º 1/2005, de 10 de janeiro, alterada e republicada pela Lei n.º 9/2012, de 23 de fevereiro (doravante, Lei n.º 1/2005), que regula a utilização de câmaras de vídeo pelas forças e serviços de segurança em locais públicos de utilização comum, para captação e gravação de imagem e som e seu posterior tratamento.

3. O pedido vem acompanhado de um documento do qual consta a fundamentação do requerimento e a informação técnica do sistema, doravante designado por "Fundamentação", bem como a avaliação de impacto sobre a proteção de dados (AIPD). A solicitação da CNPD, foram prestados esclarecimentos adicionais sobre alguns aspetos técnicos do sistema de videovigilância.

## II. Apreciação

### i. Objeto do parecer a emitir nos termos do artigo 3.º da Lei n.º 1/2005, de 10 de janeiro

4. Nos termos do n.º 2 do artigo 3.º da Lei n.º 1/2005, o parecer da CNPD restringe-se à pronúncia sobre a conformidade do pedido com as regras referentes à segurança do tratamento dos dados recolhidos, bem como acerca das medidas especiais de segurança a implementar adequadas a garantir os controlos de entrada nas instalações, dos suportes de dados, da inserção, da utilização, de acesso, da transmissão, da introdução e do transporte e, bem como à verificação do cumprimento do dever de informação e perante quem os direitos de acesso e retificação podem ser exercidos.

5. De acordo com o disposto no mesmo preceito legal e nos n.ºs 4, 6 e 7 do artigo 7.º daquela lei, é também objeto do parecer da CNPD o respeito pela proibição de instalação de câmaras fixas em áreas que, apesar de situadas em locais públicos, sejam, pela sua natureza, destinadas a ser utilizadas em resguardo ou a utilização de câmaras de vídeo quando a captação de imagens e de sons abranja interior de casa ou edifício habitado ou sua dependência, ou quando essa captação afete, de forma direta e imediata, a intimidade das pessoas, ou resulte na gravação de conversas de natureza privada.

6. Deve ainda a CNPD verificar se estão assegurados, a todas as pessoas que figurem em gravações obtidas de acordo com a presente lei, os direitos de acesso e eliminação, com as exceções previstas na lei.

7. Nos termos do n.º 7 do artigo 3.º do mesmo diploma legal, pode também a CNPD formular recomendações tendo em vista assegurar as finalidades previstas na lei, sujeitando a emissão de parecer totalmente positivo à verificação da completude do cumprimento das suas recomendações.

### ii. A finalidade do tratamento decorrente da videovigilância em locais públicos de utilização comum na cidade de Santarém

8. Pretende-se a instalação de um sistema de videovigilância composto por 26 câmaras na cidade de Santarém, mais especificamente no centro histórico da cidade, no jardim das Portas do Sol e estacionamento da estação ferroviária.

9. Implicando a instalação e funcionamento de um sistema de videovigilância na cidade de Santarém um tratamento de dados pessoais que, pelo seu âmbito, é suscetível de afetar significativamente a vida privada das pessoas que aí circulem ou se encontrem, importa considerar a finalidade da utilização do sistema.

10. Da Fundamentação que acompanha o pedido decorre que a finalidade é a proteção de pessoas e bens, públicos e privados, e prevenção da prática de factos qualificados pela lei como crimes, em locais em que exista razoável risco da sua ocorrência, nos termos das alíneas *c)* do n.º do artigo 2.º da Lei n.º 1/2005.

11. Ainda quanto aos aspetos gerais do tratamento de dados pessoais, importa atentar no impacto do mesmo sobre a privacidade dos cidadãos. Ainda que se pretenda que as câmaras que compõem o sistema de videovigilância sejam «orientadas somente para os espaços de utilização comum» (como é sublinhado na AIPD), a verdade é que existe o risco de captação de imagens de bem como espaços públicos de lazer, bem como de edifícios destinados à habitação (como é reconhecido na AIPD) e, em todo o caso, edifícios e espaços privados, dentro dos quais as pessoas têm o direito e a expetativa de que a sua privacidade seja salvaguardada.

12. Todavia, não há na Fundamentação referência expressa a esse risco e a medidas destinadas a mitigá-lo, para além da aplicação de um sombreado sobre alguns edifícios nos fotogramas que parecem representar máscaras. Estranha-se também que na AIPD se afirme existirem na zona urbana onde o sistema vai ser instalado edifícios de habitação e, depois, se omita tal facto na identificação dos riscos, prevendo-se como medida mitigadora do risco «médio» de «excesso de recolha» de dados que as «câmaras estão orientadas somente para os espaços de utilização comum».

13. Recorda-se que, apesar de não caber, nos termos das competências legais definidas na Lei n.º 1/2005, à CNPD pronunciar-se sobre a proporcionalidade da utilização de sistemas de videovigilância em locais públicos

de utilização comum, essa competência já existe quando em causa estejam câmaras instaladas em áreas que sejam, pela sua natureza, destinadas a ser utilizadas em resguardo, as câmaras captem imagens do interior de casas de habitação, ou a captação de imagens ou som afete, de forma direta e imediata, a intimidade das pessoas, ou resulte na gravação de conversas de natureza privada (cf. n.ºs 4, 6 e 7 do artigo 7.º da Lei n.º 1/2005).

14. Ora, no caso concreto, além do âmbito do tratamento de dados pessoais, deve aqui considerar-se ainda que algumas dessas câmaras têm capacidade de rotação e ampliação da imagem, o que significa a capacidade de captar, em todas as direções e com grande acuidade, imagens de pessoas.

15. Assim, não estando suficientemente descritas as situações e termos em que terá lugar a aplicação de máscaras, nem se haverá ou não possibilidade de as alterar ou eliminar, a CNPD não pode ajuizar sobre a proporcionalidade do tratamento de dados pessoais nos termos dos n.ºs 6 e 7 do artigo 7.º da Lei n.º 1/2005. Insiste-se que a captação de imagens de pessoas em suas casas e em espaços que merecem resguardo impactam de sobremaneira na privacidade, não podendo ficar dependentes de critérios subjetivos do agente que no momento esteja a operar o sistema, reclamando, por isso mesmo, orientações precisas e específicas.

16. Quanto à funcionalidade de captação de som, declara-se na primeira parte do pedido que «o sistema de videovigilância apenas se destina à captação de imagem, não havendo lugar à captação/gravação de som». Isso mesmo foi confirmado em sede de esclarecimentos solicitados pela CNPD, apesar de algumas câmaras terem aptidão para captar e gravar som e apesar de no ponto 13 do anexo F se admitir «que o sistema não possibilita a captação de som, exceto nas situações devidamente previstas na Lei e devidamente autorizadas». Uma vez que não há intenção de utilizar tal funcionalidade, opção que a CNPD louva tendo em conta que há captação de espaços públicos de lazer onde o risco de captação de conversas de natureza privada é maior, a CNPD recomenda que sejam adotadas medidas adequadas a garantir que a mesma não seja acionável por qualquer operador.

### iii. Responsável pelo tratamento

17. A CNPD destaca também que o responsável pelo tratamento de dados pessoais só pode ser a PSP, estranhando-se por isso que, no Anexo C da Fundamentação, venha essa responsabilidade imputada também ao Encarregado de Proteção de Dados. Com efeito, aí se declara que a conservação e o tratamento dos dados recolhidos através do sistema de videovigilância são da responsabilidade «de Encarregado de Proteção de Dados» (e que aí se identifica), para além de «PSP – Chefe da Área Operacional do Comando Distrital de Santarém».

18. Sublinha-se que a intervenção do Encarregado de Proteção de Dados em todos estes procedimentos só pode ser consultiva ou de controlo, não dispondo ele, nos termos da lei, de poderes de decisão sobre o tratamento de dados pessoais e, por isso mesmo, não lhe podendo ser imputada responsabilidade pela sua realização (cf. artigo 35.º da Lei n.º 59/2019, de 8 de agosto).

### iv. Subcontratação

19. Em relação à instalação e manutenção do sistema de videovigilância, porque ela está diretamente relacionada com a segurança da informação e a aptidão do sistema para cumprir as finalidades visadas, importa sublinhar que essa obrigação recai sobre o responsável pelo tratamento de dados, independentemente de quem seja o proprietário das câmaras de vídeo e demais equipamentos que componham o sistema.

20. Estabelecendo a Lei n.º 1/2005, no n.º 2 do artigo 2.º, que o responsável pelo tratamento dos dados *é a força de segurança com jurisdição na área de captação ou o serviço de segurança requerente*, eventual subcontratação em empresa para assegurar a manutenção ou substituição dos equipamentos tem de ser formalizada, contratualmente, com a PSP. Não está afastada a hipótese de a PSP subcontratar o Município de Leiria, podendo esta subsubcontratar empresas, nos termos regulados no artigo 23.º da Lei n.º 59/2019, de 8 de agosto. O que não pode é haver uma inversão de papéis, ficando a PSP sem o domínio ou controlo do tratamento de dados pessoais que o sistema de videovigilância realiza.

21. A CNPD insiste neste ponto, essencial no âmbito do tratamento de dados pessoais a realizar, uma vez que os n.ºs 1 e 5 da Cláusula Segunda do Protocolo celebrado entre a PSP e o Município de Santarém (cf. Anexo J) refletem uma conceção da relação jurídica e das obrigações das partes que não é compatível com o regime legal de proteção de dados pessoais. Na verdade, quer a definição dos meios a utilizar para o tratamento de dados pessoais e, especificamente, as suas características de modo a cumprir os requisitos técnicos regulamentarmente impostos, quer o pedido de autorização par a instalação do sistema de videovigilância é exclusivamente da competência da PSP, por, precisamente nos termos da lei, ser esta entidade a responsável pelo tratamento de dados pessoais.

22. Importa, por isso, que seja celebrado um contrato ou acordo que regule especificamente essa relação de subcontratação, vinculando o Município nos termos do artigo 23.º da Lei n.º 59/2019 – o que no caso concreto não parece ocorrer, uma vez que o texto do protocolo anexado à Fundamentação é manifestamente insuficiente nesta perspetiva.

23. Especificamente quanto às subsubcontratações, recorda-se que nos termos do mesmo artigo 23.º, elas dependem de autorização prévia do responsável.

v. Segurança do sistema de videovigilância

24. No anexo B indica-se que o local de visualização das imagens é o Centro de Comando e Controlo situado nas instalações do Comando Distrital de Santarém da PSP. Quanto ao controlo de acessos, especifica-se ser esse um espaço de acesso restrito aos operadores de comunicação, devidamente credenciados, admitindo-se ainda o acesso por outras pessoas, mediante solicitação e motivo de serviço que o justifique.

25. Também especificamente quanto ao compartimento condicionado onde se procede à gravação dos dados, prevê-se, no anexo F da Fundamentação, «um sistema de controlo de acessos que somente permita a entrada, sem acompanhamento, de pessoas devidamente habilitadas e autorizadas; quanto às restantes pessoas, os acompanhantes devem-nas impedir de ter acesso aos produtos ali armazenados», prevendo-se ainda o registo de acessos. Mais se refere que o acesso a esse compartimento depende de uma chave guardada em envelope lacrado, acessível apenas ao pessoal adstrito a funções no sistema de videovigilância.

26. A CNPD sublinha a importância de o mecanismo de controlo de acessos ter aptidão para registar, além das entradas, também as saídas. Só desse modo, é possível demonstrar a imputabilidade subjetiva de qualquer evento. Sugere-se o reforço da segurança nos acessos a estes espaços com um sistema automático de 2 fatores (*v.g.*, *smartcard*, código *pin*, *token*), personalizado a cada operador e que permita rastrear a todo o tempo as entradas, saídas e quem estava presente na sala em determinado instante.

27. Já em relação ao registo de pessoas não credenciadas, uma vez que esse registo depende da ação de um elemento credenciado, assinala-se a necessidade de adoção de uma solução que não permita falhas ou omissões na inscrição daquelas pessoas.

28. Quanto à solução supletiva de a chave de acesso ao compartimento ser conservada em envelope lacrado, afirma-se, no Anexo F, que a «abertura do envelope implica sempre a elaboração de informação justificativa do respetivo motivo, procedendo-se no mais curto prazo ao acondicionamento da chave em novo envelope lacrado, datado e assinado pelo responsável pela conservação e tratamento dos dados». Como a substituição da chave de acesso parece estar limitada às situações de em que haja «quebra de segurança ou se suspeite dessa possibilidade», a medida prevista de (re)armazenamento da chave de acesso em novo envelope não é suficiente para garantir a confidencialidade da chave de acesso e, consequentemente, da integridade das imagens gravadas. Assim, a CNPD recomenda que, sempre que haja necessidade de abrir o envelope, seja substituída a chave de acesso.

29. Nos esclarecimentos adicionais solicitados pela CNPD, vem indicado que «a ligação ao parque de estacionamento da estação ferroviária de Santarém é efetuada através de um link ponto a ponto wireless», com configuração de uma ligação ponto-a-ponto com o terminal e possível proteção por *MAC address* e

encriptação WPA2-AES. Alerta-se que uma estação é local público de passagem com bastante afluência de pessoas e, portanto, bastante exposto, sugerindo-se constante monitorização e configuração de alertas para detetar anomalias ou intrusão na rede *wireless* por onde se expõe a VLAN do sistema de videovigilância.

30. Nos esclarecimentos adicionais consta também que «o acesso à consola das câmaras está na rede de videovigilância e somente poderá ser acedida por um equipamento dedicados ao sistema, os quais serão os gravadores e posto de visualização na sala do Centro de Comando e Controlo Operacional. Os protocolos não usados e prescindíveis ao funcionamento da solução serão desabilitados.». Foram ainda prestados esclarecimentos adicionais relativamente à a arquitetura lógica da rede.

31. A CNPD entende que o enquadramento aí descrito tem as condições para garantir a segurança das comunicações do sistema de videovigilância, desde que se assuma o compromisso de, além da desativação nas câmaras dos protocolos de comunicação não utilizados, se alterarem as credenciais de *login* e *password* para autenticação forte e com uma política de gestão de senhas.

32. Ainda no contexto da segurança do sistema, importa sublinhar que os armários de distribuição das telecomunicações, a instalar no espaço público, não devem estar acessíveis a qualquer pessoa, sobretudo pelo risco de atos de vandalismo ou ações intencionais de ataque ao sistema, como por exemplo desligar câmaras para impedir filmagem de atos ilícitos planeados. É, por isso, essencial que não estejam localizados no chão ou a uma altura que os torne facilmente acessíveis e que disponham de um sistema de alerta/alarme em caso de acesso indevido por terceiros.

33. Por fim, assinala-se que de nada serve ter uma rede segregada e isolada se pontualmente for aberto um canal de comunicação na Internet, expondo desse modo o sistema às vulnerabilidades de uma rede aberta. Com efeito, é essencial garantir que os serviços de suporte e manutenção ao sistema de videovigilância sejam prestados fisicamente no local, não sendo admissível o acesso remoto na medida em que este pode comprometer a segurança.

### vi. Integridade e auditabilidade do tratamento de dados pessoais

34. Quanto a este ponto, a CNPD recomenda somente que seja definida uma política de retenção dos registos de rastreabilidade e indicadores chave para os relatórios de auditoria, em sede de monitorização da segurança nos acessos e das operações efetuadas, sublinhando a importância de que os registos cronológicos sejam objeto regular de análise, sob pena de não cumprirem a sua função de possibilitar a deteção de falhas e anomalias

35. Deste modo, alerta-se para a imprescindibilidade de o responsável pelo tratamento, ou seja, a PSP, estar dotado de recursos humanos com conhecimentos técnicos suficientes para analisar os registos e identificar eventuais incidentes.

## III. Conclusão

36. Não cabendo na competência que lhe está legalmente atribuída pronunciar-se sobre a proporcionalidade da instalação de um sistema de videovigilância na cidade de Santarém, a CNPD, com os argumentos acima expostos:

a. Sublinha que a captação de imagens de pessoas em suas casas, não podendo ficar dependentes de critérios subjetivos do agente que no momento esteja a operar o sistema de videovigilância, reclamando, por isso mesmo, orientações precisas – na sua falta, ou na falta de informação à CNPD sobre as mesmas, a CNPD não pode concluir o seu juízo sobre o cumprimento dos requisitos do artigo 7.º da Lei n.º 1/2005;

b. Alerta para a inadmissibilidade de se considerar como responsável pelo tratamento o Encarregado de Proteção de Dados (EPD), pois que em todos os tratamentos de dados pessoais, a intervenção do EPD só pode ser consultiva ou de controlo, não dispondo ele, nos termos da lei, de poderes de decisão sobre o tratamento de dados pessoais e, por isso mesmo, não lhe podendo ser imputada responsabilidade pela sua realização;

c. E insiste que, sendo o responsável pelo tratamento de dados pessoais, nos termos da lei, a PSP, tem de ficar expressa e claramente delimitada em contrato ou acordo a intervenção do Município como subcontratante desta entidade, bem como de eventuais subsubcontratantes.

37. Quanto à segurança do sistema, da integridade e de auditabilidade do tratamento de dados pessoais, a CNPD limita-se a recomendar a adoção de um conjunto de medidas, nos termos especificados supra, nos pontos 28 a 35.

Lisboa, 7 de julho de 2021

Filipa Calvão (Presidente, que relatou)