

PARECER/2021/92

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 do Funchal, 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 do Funchal

8. Pretende-se a instalação de um sistema de videovigilância composto por 81 câmaras, sendo 65 fixas e 16 rotativas, na cidade do Funchal, mais especificamente na baixa da cidade, na marginal e entre o parque municipal e o mercado municipal.

9. Implicando a instalação e funcionamento de um sistema de videovigilância na cidade do Funchal um tratamento de dados pessoais que, pelo seu âmbito e extensão, 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. Na Fundamentação que acompanha o pedido, declara-se que a finalidade «designadamente 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. No entanto, e porque ao caracterizar-se a finalidade do tratamento se utiliza advérbio *designadamente*, a CNPD recorda que, embora a lei, no n.º 1 do citado artigo 2.º, admita outras finalidades, na medida em que se identifica somente a finalidade de proteção de pessoas e bens e de prevenção criminal, não pode o sistema de videovigilância ser utilizado para outras finalidades enquanto tal não for objeto da correspondente autorização.

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 edifícios destinados à habitação e, em todo o caso, edifícios e espaços privados, dentro dos quais as pessoas têm o direito e a expectativa 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 sinalização de máscaras em alguns fotogramas, constando apenas da AIPD a menção de criação de «zonas de bloqueio digital de gravação através da programação do software da própria câmara».

13. Recordar-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 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 e 7 do artigo 7.º da Lei n.º 1/2005).

14. Ora, no caso concreto, para além da extensão 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, a que acresce a possibilidade de captação de som.

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 do artigo 7.º da Lei n.º 1/2005.

16. Acrescente-se também, quando à funcionalidade de captação de som, que não está explicado como se garante «que o sistema não possibilita a captação de som, exceto nas situações devidamente previstas na Lei e devidamente autorizadas» – pois ou sistema não tem essa funcionalidade, ou o sistema integra tal funcionalidade, caso em que têm de ser especificadas as circunstâncias da sua utilização.

17. Insiste-se que a captação de som e 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.

18. Ainda em sede de considerações gerais sobre o tratamento de dados pessoais decorrente da utilização de um sistema de videovigilância, realça-se que, não obstante os esclarecimentos adicionais prestados, há aspetos do tratamento sobre os quais a CNPD não pode concluir a sua avaliação por falta de elementos mais precisos.

19. Tal sucede, desde logo, quanto ao eventual recurso a tecnologias de inteligência artificial. Ainda que se tenha declarado, em sede dos referidos esclarecimentos adicionais, que «apesar da possibilidade apresentada não será utilizado nenhum sistema de reconhecimento facial», fica por esclarecer se as soluções finais a implementar permitem ainda, e em que condições, o rastreamento de pessoas e viaturas. Não estando



especificamente descrita tal funcionalidade no pedido e não sendo, por isso, possível avaliar o seu impacto sobre os direitos dos cidadãos, deve essa possibilidade ficar claramente vedada.

20. Finalmente, assinala-se que sendo o pedido, apesar dos esclarecimentos adicionais, ainda incompleto quanto à caracterização técnica da solução para o sistema a implementar, uma vez que está esboçado com referências genéricas a produtos de fabricantes do setor, sem valor vinculativo, a CNPD não consegue concluir se serão adotadas todas as medidas necessárias a garantir a segurança do sistema de videovigilância e de integridade e auditabilidade do tratamento de dados pessoais.

21. Em face disso, algumas das observações da CNPD terão em vista contribuir para a especificação do caderno de encargos para adjudicação da implementação do sistema de videovigilância, de modo a garantir que a concretização da solução técnica não implique riscos acrescidos para os dados pessoais e os direitos dos cidadãos.

iii. Responsável pelo tratamento

22. A CNPD destaca ainda 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 Regional da Madeira».

23. 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

24. 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.

25. 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.

26. Importa, por isso, que seja celebrado um contrato ou acordo que regule especificamente essa relação de subcontratação, vinculando o Município nos termos daquela norma legal – o que no caso concreto não parece ocorrer, uma vez que o texto do protocolo anexado à Fundamentação é insuficiente nesta perspetiva.

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

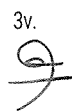
v. Segurança do sistema de videovigilância

28. No anexo B são indicados dois locais físicos de agregação de dados: o centro de processamento de dados nos Paços do Concelho e o Comando Regional da Madeira da PSP. Do anexo F decorre que existirá um compartimento de acesso condicionado para os meios físicos de suporte à gravação de dados registados. No ofício que integra esclarecimentos adicionais consta que «nos Paços do Concelho apenas ficarão os ativos de comunicação, não havendo qualquer captação de dados, sendo que o servidor com tratamento de dados, visualização e postos de trabalho ficarão localizados exclusivamente no centro de comando e controlo operacional da PSP».

29. Por conseguinte, recomenda-se que os ativos de comunicação a alojar nos Paços do Concelho fiquem em infraestrutura segregada da restante do centro de processamento de dados do Município, se possível em bastidores separados e protegidos por uma “jaula” com chave, acessível apenas a pessoal credenciado para realizar intervenções de manutenção ao sistema de videovigilância.

30. Quanto ao controlo de acessos no Centro de Comando e Controlo do Comando Regional da Madeira, onde estarão instalados os ecrãs de monitorização, 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.

31. 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.

32. Em resposta ao pedido de esclarecimentos adicionais, foi especificado que será implementado um sistema de controlo que garanta a «verificação a todo o tempo das entradas, saídas de quem esteve presente nos espaços em determinado instante. A utilização de chave, será apenas em última instância se ocorrer um corte de energia geral, embora o Comando Regional esteja equipado com um grupo gerador de emergência».

33. 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. Acresce que este mecanismo deve exigir dois fatores de autenticação.

34. 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.

35. Já quanto 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.

36. Solicitado esclarecimento se o acesso à consola das câmaras está disponível na rede e se é acessível a partir de um outro equipamento na mesma rede, como por exemplo no ponto de agregação dos dados situados nos paços do concelho, a resposta foi que «todas as câmaras serão protegidas com *username* e *password*, sendo apenas acessíveis no centro de comando e controlo operacional da PSP».

37. Recomenda-se que se defina uma arquitetura lógica de rede em que não seja possível ligar equipamentos informáticos aos ativos de comunicação e aceder às consolas *Web* das câmaras. Deve ainda definir-se uma política de autenticação segura para os acessos a atribuir a cada uma das consolas dos equipamentos, que previna a hipótese de uma credencial única comum para todos os equipamentos.

38. Ainda no contexto da segurança do sistema, são indicados 32 armários de distribuição das telecomunicações, cada um deles agregando várias câmaras na proximidade. Em sede de esclarecimentos adicionais declarou-se que «os armários terão proteção reforçada anti-intrusão, bem como sistema de alerta/alarme em caso de arrombamento ligado ao centro de comando e controlo da PSP». Sublinha-se ainda ser fundamental garantir que os armários de distribuição das telecomunicações – portanto, instalados no espaço público – não estejam 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.

39. 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

40. Para efeito de investigação criminal, prevê-se um processo de extração de imagens, «quando haja notificação para preservação das mesmas nos termos do art.º 55 Código de Processo Penal, e ou por solicitação direta e formal das Autoridades Judiciárias».

41. Importa, a este propósito, sublinhar que o *software* de gestão do sistema de videovigilância tem de dispor de mecanismos que viabilizam a exportação em formato digital, assinado digitalmente, que ateste a veracidade do seu conteúdo. E devem ainda prever-se mecanismos de cifra, caso se pretenda proteger a exportação, no contexto da, com uma senha de acesso ou outro fator de segurança.

42. Na AIPD, constante do anexo J da Fundamentação, afirma-se que «o acesso às imagens gravadas será realizado apenas por polícias autorizados e credenciados para o efeito e por motivos previstos na Lei. Cada utilizador autorizado terá um perfil autónomo no servidor de vídeo que permita rastrear todas as ações que realizou no sistema». Por sua vez, no anexo F refere-se «Todas as intervenções realizadas ao nível dos (sistemas locais) são registadas em formato digital, de forma encriptada, em tempo real e de forma que sejam auditáveis, devendo o sistema de registo de eventos estar sempre ativo, a fim de permitir as referidas operações de auditoria».



43. Dá-se nota de que, para que um sistema seja verdadeiramente auditável, é imperativo garantir que o mesmo tem o detalhe da operação realizada, para que seja possível a todo o momento saber *quem* e *o que* fez sobre os dados pessoais. Aliás, nesse mesmo sentido aponta a Resolução do Conselho de Ministros n.º 41/2018, de 28 de março, a qual determina a implementação também deste requisito por parte dos serviços da Administração Estadual Direta e Indireta. Aí se prevê a obrigação de registo de todas as ações que um utilizador efetue sobre dados pessoais, incluindo tentativas de acesso, bem como a obrigação de garantia da sua integridade, através de assinatura digital e *TimeStamp*.

44. Para melhor compreensão do que se está a dizer, tome-se o seguinte exemplo: não basta registar que houve uma ação sobre uma máscara na imagem captada, sendo necessário especificar se esta foi colocada, retirada ou alterada.

45. Nos esclarecimentos adicionais, precisou-se que os registos terão selo temporal (*timestamp*) e que a encriptação será definida no software a adquirir de forma que fique disponível apenas e só a pessoas credenciadas.

46. A CNPD recomenda 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

47. 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

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


- a. Sublinha que a captação de som e 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 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.

49. Uma vez que o pedido, e demais informação prestada, é omissivo quanto a alguns elementos de caracterização técnica do sistema de videovigilância, a CNPD não pode proceder a uma avaliação completa da segurança do sistema e ainda da integridade e auditabilidade do tratamento de dados pessoais, pelo que se limita a recomendar a adoção de um conjunto de medidas, nos termos especificados supra, nos pontos 28 a 47.

Lisboa, 5 de julho de 2021



Ana Paula Lourenço (Relatora)