CNPD
Comissão Nacional
de Proteção de Dados

PARECER/2021/110

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 para instalação e utilização de um sistema de videovigilância na cidade da Figueira da Foz, 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 pedido e a informação técnica do sistema, doravante designado por "Fundamentação", bem como a avaliação de impacto sobre a proteção de dados (AIPD).

4. A solicitação da CNPD, foram ainda prestados esclarecimentos adicionais relativamente a alguns aspetos do sistema que estavam omissos ou incompletos no texto da Fundamentação.

II. Apreciação

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

5. 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.

6. 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.

7. 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.

8. 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. As finalidades do tratamento decorrente da Videovigilância em locais públicos de utilização na cidade da Figueira da Foz

9. Não obstante 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).

10. Ora, a instalação e utilização de um sistema de videovigilância na cidade da Figueira da Foz, especificamente «*na área central da cidade da Figueira da Foz, comummente designada por Bairro Novo*», implica um tratamento de dados pessoais suscetível de afetar significativamente a vida privada das pessoas que aí circulem ou se encontrem.

11. Em causa está a instalação e utilização de 12 câmaras numa área que é considerada, no pedido, como «[...] *de ocupação predominantemente comercial (restauração, bares, bem como discotecas) com ocupação residencial diminuta ao nível dos residentes fixos, no entanto, localizam-se nesta zona e arredores vários hotéis e pensões, as quais durante o período estival e festivos [...] se encontram lotados com turistas e público*». (cf. ponto 2.a. da Fundamentação que acompanha o pedido).

12. Das 12 câmaras, 3 têm funcionalidades de PTZ (*Pan, Tilt e Zoom*), o que significa a capacidade de captar, em todas as direções e com grande acuidade, imagens de pessoas e veículos, a que acresce a possibilidade de captação de som por todas as câmaras – declarando-se, aliás, que todas as câmaras procederão à captação e gravação de som (cf. ponto 3. da Fundamentação).

13. Importa também assinalar que a captação e gravação de imagens e som é, de acordo com o pedido, temporalmente delimitada: ocorrerá entre as 18h e as 8h do dia seguinte, estando limitada aos seguintes períodos:

a. Desde a sexta-feira anterior ao dia de carnaval até quarta-feira de cinzas;

b. 01 de junho a 15 de setembro;

c. De 15 a 31 de dezembro;

d. De 01 de janeiro até ao primeiro dia útil do ano;

e. Desde a sexta-feira que antecede a Sexta-Feira Santa até á segunda-feira após o domingo de Páscoa,

f. Sem prejuízo dos períodos anteriores, às sextas-feiras e aos sábados e nos dias vésperas de feriado nacional ou local. (cf. ponto 3. da Fundamentação).

14. Recorda-se que o tratamento de dados tem, de acordo com o declarado, a finalidade de 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 da alínea *c)* do n.º do artigo 2.º da Lei n.º 1/2005.

15. Na Fundamentação, prevê-se a adoção de medidas destinadas a salvaguardar a privacidade das pessoas dentro dos edifícios, através da aplicação de filtros de imagens, o que mitiga substancialmente o impacto sobre os direitos dessas pessoas. Esses filtros ou máscaras vêm representados no Anexo A da Fundamentação, e no Anexo B esclarece-se que todas as câmaras são compatíveis «[...] *com configurações de compressão e qualidade de imagem e ter zonas de máscaras de privacidade [...], bem como ser compatível com máscaras de privacidade em 3D individualmente configuráveis*», «[...] *as quais serão dinamicamente ajustadas com base no fator de zoom atual, e o operador não conseguirá exibir os conteúdos protegidos*».

16. Já quanto à captação e gravação de som, não encontra a CNPD qualquer fundamento específico em todo o pedido e respetiva fundamentação, tão-pouco na AIPD que acompanha aquele.

17. Insiste-se que a captação e gravação de som, nas imediações de casas de habitação, mas também em espaços públicos, impactam de sobremaneira na privacidade, não devendo ocorrer salvo se se demonstrar a sua imprescindibilidade para a finalidade visada com este tratamento de dados – o que manifestamente aqui não ocorre.

18. Demais, a gravação de som no contexto acima descrito afigura-se ser, em todo o caso, desproporcionada, por nem sequer se revelar adequada à finalidade de proteção de pessoas e bens, menos ainda à prevenção de qualquer crime. Aliás, tendo em conta as zonas abrangidas pelo sistema de videovigilância e os períodos em que se pretende utilizá-lo é evidentemente elevado o risco de gravação de conversas privadas, o que é expressamente proibido no n.º 7 do artigo 7.º, *in fine*, da Lei n.º 1/2005.

19. A CNPD entende, assim, não haver fundamento que legitime a gravação de som no espaço público (desde logo, nas imediações de edifícios destinados a habitação), sob pena de violação do n.º 7 do artigo 7.º da Lei n.º 1/2005, e recomenda que seja especialmente ponderada a autorização da captação permanente de som, por não estar demonstrada a necessidade desse tratamento de dados pessoais para a finalidade visada. Mesmo a pontual captação de som, a ser autorizada, deve ser enquadrada por orientações precisas, não podendo ficar dependente de critérios subjetivos do agente que no momento esteja a operar o sistema.

iii. Subcontratação

20. 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.

21. 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 da Figueira da Foz, 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.

22. 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.

23. Considerando ainda que, de acordo com os esclarecimentos adicionais prestados, a transmissão das câmaras será «*através de uma estrutura dedicada de fibra ótica, a operar exclusivamente com o sistema, desde o local onde as câmaras serão montadas até às instalações do Comando Distrital de Coimbra da PSP*», especificamente, «*com recurso a uma estrutura de fibra ótica dedicada*», dificilmente poderá ser o Município da Figueira da Foz, mesmo na qualidade de subcontratante, a assumir tal tarefa, dados os limites territoriais das suas atribuições, pelo que se afigura provável o recurso pela PSP a mais subcontratantes.

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

iv. Aptidão do sistema de videovigilância para reconhecimento facial e rastreamento dos cidadãos

25. No anexo B é indicado como fabricante dos componentes do sistema de videovigilância a empresa Avigilon, assim como o *software Control Center*. Este *software* traz inúmeras funcionalidade de Inteligência Artificial (IA). Nomeadamente, tecnologia de reconhecimento facial para identificar pessoas de interesse com base em uma ou mais listas de observação e também um mecanismo para examinar horas de vídeo gravado com facilidade de localizar rapidamente uma pessoa ou veículo de interesse. Nos esclarecimentos adicionais, declarou-se que «*tais capacidades não serão utilizadas e ficarão desligadas*».

26. Assinala-se, contudo, que as funcionalidades, ainda que desligadas, permanecem disponíveis no referido *software* e, portanto, são suscetíveis de ativação pelo menos pelo perfil de administrador. Tendo em conta o impacto da sua utilização na privacidade dos cidadãos, importa garantir que não serão ativadas. Recomenda-se, assim, que em eventual decisão autorizativa sobre a instalação e utilização deste sistema de videovigilância seja proibida expressamente a ativação das funcionalidades de IA que permitem o reconhecimento facial e o rastreamento dos cidadãos.

v. Segurança do sistema de videovigilância

27. Na perspetiva da segurança do sistema de videovigilância, sobre a instalação física das câmaras consta dos esclarecimentos adicionais que «*as câmaras serão afixadas nas fachadas dos edifícios existentes nos locais indicados, inseridas em caixas próprias para o efeito, que conferem proteção antivandalismo*». Não é referido um mecanismo de natureza "anti-tampering" nas caixas, com alertas. Assim, recomenda-se que seja contemplada alarmística de intrusão nos armários de comunicação onde ficarão ligadas as câmaras.

28. É ainda fundamental garantir que os armários de distribuição das comunicações – 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.

29. No anexo F da Fundamentação afirma-se que «*os ecrãs de monitorização serão instalados no Centro de Comando e Controlo do Comando Distrital de Coimbra espaço cujo acesso é restrito aos operadores de comunicações, devidamente credenciados para o efeito conforme listagem aprovada* [...] *O acesso ao Centro de Comando e Controlo e aos ecrãs de monitorização por elementos que não os referidos operadores de comunicações só é permitido mediante solicitação e motivo de serviço que o justifique*». O mesmo anexo informa que a *gravação dos dados registados será efetuada através de meios físicos instalados em*

compartimento condicionado, no Comando Distrital de Coimbra com acesso condicionado, prevendo-se o estabelecimento de um sistema de controlo de acesso que somente permita a entrada, sem acompanhamento, de pessoas devidamente habilitadas e autorizadas». Nos esclarecimentos adicionais, acrescenta-se que «*ambos os espaços vão estar localizados numa área de segurança classe 1, cujo acesso possui já 2 níveis de controlo (portas apenas acessíveis com cartão individual programada - passível de ser rastreada e, em seguida, portas diferenciadas por serviço, apenas acessível com chave física)*».

30. Do declarado depreende-se que o acesso ao espaço de cada serviço, dentro da área de segurança de classe 1, é feita através de uma chave física, o que não parece permitir aferir com exatidão quem está presente em dado momento em cada serviço, dentro da referida área de segurança. Seria preferível adotar a lógica inversa, utilizando uma chave física para aceder à área de segurança e, depois, o cartão individual para entrar no específico serviço pretendido.

31. Acresce que o mecanismo de controlo do acesso pelas pessoas autorizadas deve – para ser plenamente apto a identificar quem, em cada momento, se encontra nas duas salas – registar, além das entradas, também as saídas. Só desse modo, é possível demonstrar a imputabilidade subjetiva de qualquer evento.

32. Quanto ao registo de pessoas não credenciadas, mencionado no Anexo F da Fundamentação, uma vez que o mesmo depende da ação de elemento credenciado, assinala-se a necessidade de adoção de uma solução que não permita falhas ou omissões na inscrição daquelas pessoas.

33. Finalmente, assinala-se que não foram prestadas informações suficientes sobre o procedimento de extração de imagens para efeito de investigação criminal. Em especial, importa definir regras sobre o procedimento de preservação das imagens extraídas, que garantam a sua eliminação após a conclusão do processo-crime.

vi. Auditabilidade do tratamento de dados pessoais

34. Quanto à previsão da existência de registos cronológicos, no Anexo G da Fundamentação, dá-se nota de que não basta a afirmação genérica de que a aplicação deverá guardar em memória as atividades do sistema. Com efeito, 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.

35. 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*.

36. Para melhor compreensão do que se está a dizer, exemplifica-se não ser bastante registar que houve uma ação sobre uma máscara, sendo necessário especificar se esta foi colocada, retirada ou alterada.

37. Deverá ser definida uma política de retenção dos registos de atividade (i.e., por quanto tempo são retidos até serem descartados) e indicadores chave para os relatórios de auditoria em sede de monitorização da segurança nos acessos e das operações efetuadas

38. Finalmente, importa ainda atender ao facto de os registos cronológicos (*logs*) serem fundamentais para que se possam detetar falhas e anomalias. Porém, esta função dos registos cronológicos só é atingida se os mesmos forem objeto de análise.

39. Para o efeito, deverá ser definida uma política de retenção dos registos de atividade (*i.e.*, por quanto tempo são retidos até serem descartados) e indicadores chave para os relatórios de auditoria em sede de monitorização da segurança nos acessos e das operações efetuadas.

40. 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

41. Não cabendo na competência que lhe está legalmente atribuída pronunciar-se sobre os concretos fundamentos da instalação e utilização do sistema de videovigilância na cidade da Figueira da Foz, a CNPD, com os argumentos acima expostos:

a. Entende não haver fundamento que legitime a gravação de som no espaço público (desde logo, nas imediações de edifícios destinados a habitação), sob pena de violação do n.º 7 do artigo 7.º da Lei n.º 1/2005;

b. Recomenda que seja especialmente ponderada a autorização da captação permanente de som, por não estar demonstrada a necessidade desse tratamento de dados pessoais para a finalidade visada, devendo eventual autorização de pontual captação de som ficar dependente de critérios precisos que orientem os operadores do sistema;

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, e de eventuais subsubcontratantes, bem como de outros subcontratantes;

d. Uma vez que o *software* aplicado compreende funcionalidades de Inteligência Artificial que permitem o reconhecimento facial e o rastreamento dos cidadãos, as quais, apesar de se declarar que não serão utilizadas, permanecem no sistema e são suscetíveis de utilização (pelo menos pelo perfil de administrador do sistema), recomenda-se que em eventual decisão autorizativa sobre a instalação e utilização deste sistema de videovigilância seja proibida expressamente a ativação dessas funcionalidades.

42. A CNPD recomenda ainda que sejam adotadas medidas capazes de garantir a segurança do sistema e a auditabilidade do tratamento de dados pessoais, nos termos assinalados supra, nos pontos 25 a 40.

Lisboa, 23 de agosto de 2021

Filipa Calvão (Presidente, que relatou)