

PARECER/2022/102

I. Pedido

1. Por despacho da Secretária de Estado da Administração Interna foi solicitado parecer à Comissão Nacional de Proteção de Dados (CNPDP) sobre o pedido de autorização para alargamento do sistema de videovigilância na cidade de Olhão, submetido pela Polícia de Segurança Pública (PSP).
2. O pedido de parecer foi apresentado em 30 de agosto de 2022, 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 "Fundamentação", bem como a avaliação de impacto sobre a proteção de dados (AIPD).

II. Apreciação

i. Objeto do parecer a emitir nos termos do artigo 5.º da Lei n.º 95/2021, de 29 de dezembro

4. Assim, nos termos do n.º 3 do artigo 5.º da Lei n.º 95/2021, de 29 de dezembro (doravante, Lei n.º 95/2021), o parecer da CNPDP, emitido dentro do prazo fixado no n.º 4 do mesmo artigo (em conjugação com as alíneas b) e c) do artigo 87.º do Código do Procedimento Administrativo), restringe-se à pronúncia sobre a conformidade do pedido com as regras referentes à segurança do tratamento dos dados recolhidos e com o previsto nos n.ºs 4 a 6 do artigo 4.º e nos artigos 16.º, 18.º a 20.º e 22.º do mesmo diploma legal.
5. De acordo com o disposto nestes artigos, é também objeto do parecer da CNPDP o respeito pela 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 interior de casa ou edifício habitado 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.
6. É igualmente objeto de parecer da CNPDP 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.

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

ii. O âmbito e as finalidades do tratamento decorrente da videovigilância na cidade de Olhão

8. Não obstante não caber, nos termos das competências definidas na Lei n.º 95/2021, 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 quando aquelas captem imagens e som do interior de casa ou edifício habitado ou sua dependência ou de estabelecimentos hoteleiros e similares, ou quando a captação de imagens ou som afete, de forma direta e imediata, a esfera da reserva da vida íntima e privada (cf. n.ºs 4 a 6 do artigo 4.º da Lei n.º 95/2021).

9. Em causa está um tratamento de dados decorrente do alargamento do sistema de videovigilância na cidade de Olhão. O sistema é atualmente composto por 26 câmaras instaladas na zona da baixa da cidade de Olhão, pretendendo-se agora, de acordo com o declarado, a sua ampliação com 38 câmaras adicionais, 20 das quais a instalar na zona comercial/baixa da cidade de Olhão, e as demais (18) nos principais eixos rodoviários da cidade (cf. Anexos A, ponto 4., p. 8, da Fundamentação). Prevê-se ainda a substituição de 3 das câmaras já instaladas na zona da baixa (cf. Anexos A, ponto 4., p. 8, e D, p. 1, da Fundamentação).

10. Assim, de acordo com o declarado, pretende-se que o sistema de videovigilância na cidade de Olhão passe a integrar 64 câmaras de videovigilância, alargando substancialmente a área de captação de imagens. Todavia, no pedido refere-se um total de 67 câmaras (cf. p. 4) e, de facto, no Anexo C, contam-se 44 câmaras (26 de tipo *Bullet* e 18 multisensores). Importa, por isso, assegurar a coerência do pedido e da respetiva fundamentação, clarificando o número de câmaras a instalar e o número total de câmaras que passará a integrar o sistema de videovigilância na cidade de Olhão.

11. Assinale-se, contudo, que o número efetivo de câmaras é bem superior a esse, porquanto 18 das novas câmaras são multisensores, sendo cada uma delas composta por 4 câmaras com capacidade de funcionamento independente; o que significa que cada um dos sensores funciona, em termos práticos, como uma câmara autónoma e as imagens por si captadas são processadas e visualizadas como se de uma câmara se tratasse. Em suma, em causa estão, não apenas 18 câmaras, mas sim 72 câmaras, o que, na realidade, implica que o sistema de videovigilância da cidade de Olhão passe a integrar um total de 118, ou 121 – consoante o número efetivamente visado com o pedido, que ainda carece de clarificação – (cf. Anexo C da Fundamentação).

12. Além da significativa ampliação do âmbito territorial do sistema de videovigilância, também as finalidades do sistema são alargadas: à finalidade de proteção de pessoas, animais e bens, em locais públicos ou de acesso público, e de prevenção da prática de factos qualificados pela lei como crimes, em locais em que exista razoável risco da sua ocorrência, acrescem agora, não apenas a finalidade de resposta operacional a incidentes de segurança em curso, como também as finalidades de controlo de tráfego e segurança de pessoas, animais e bens na circulação rodoviária e a prevenção e repressão de infrações estradais, nos termos das alíneas d), f) g) e h) do n.º 1 do artigo 3.º da Lei n.º 95/2021 (cf. Anexo A da Fundamentação).

13. Contudo, as câmaras não estão especificamente adstritas a uma finalidade ou a um conjunto de finalidades. Na realidade, declara-se que as 20 câmaras a instalar na zona comercial/baixa da cidade de Olhão têm o *«objetivo primordial de proteger a segurança das pessoas e bens e prevenir a prática de crimes»*, e as 18 câmaras a instalar nos principais eixos rodoviários da cidade (Av. João VI, Av. Heróis de 1808 e o túnel rodoviário da Av. Bernardino da Silva) serão *«principalmente dirigidas à prevenção de infrações rodoviárias»* (cf. Anexo A, ponto 4., p. 8, da Fundamentação).

14. Ora, esta confusão ou partilha indiscriminada de finalidades entre as diferentes câmaras prejudica a formulação de um juízo de proporcionalidade quanto à sua utilização, porque tal juízo exige uma avaliação cuidada e ponderada da adequação, necessidade e proporcionalidade das funcionalidades de cada uma das câmaras e, em especial, do sistema de gestão analítica de dados que se pretende utilizar, em função de cada uma das finalidades declaradas – e, em rigor, algumas dessas funcionalidades ou características podem revelar-se, em concreto, desnecessárias e excessivas, ou mesmo não idóneas. Desde logo, dificilmente se pode justificar a utilização de câmaras de videovigilância nos principais eixos rodoviários da cidade com o argumento da prevenção ou combate à criminalidade; e a funcionalidade de leitura de matrículas (e do seu rastreamento) no centro da cidade afigura-se uma compressão excessiva dos direitos fundamentais à reserva da vida privada e da liberdade, pela facilidade de, a partir desse elemento informativo, se identificar o condutor.

15. Como tal, e em conformidade com a análise concretizada na AIPD (cf. p. 4), a CNPD recomenda a delimitação das finalidades do sistema pelos diferentes conjuntos de câmaras de videovigilância, em função das zonas territoriais a que respeitam e dos riscos detetados nas mesmas, de modo a permitir a avaliação da proporcionalidade pelo órgão com competência autorizativa ao abrigo do artigo 4.º da Lei n.º 95/2021, assim como da proporcionalidade do sistema de gestão analítica das imagens, ao abrigo do artigo 16.º do mesmo diploma legal.

16. Assinala-se ainda que do pedido parece resultar apenas pretender-se a gravação de imagens, portanto, sem captação e gravação de som. Não obstante, no Anexo G da Fundamentação refere-se, por duas vezes, aptidão

do sistema de gestão de analítica de dados para a análise de áudio, em tempo real e em dados gravados, o que deixa a dúvida quanto à intenção da sua utilização.

17. A CNPD sublinha que, a haver pretensão da captação de som, não foram disponibilizados à CNPD quaisquer elementos informativos que permitam avaliar do risco para a privacidade (em especial, com a utilização da tecnologia de analítica de dados), razão por que não pode aquela ser autorizada sem o competente parecer da CNPD sobre o respeito pelo limite fixado no n.º 6 do artigo 4.º da Lei n.º 95/2021, nos termos do n.º 3 do artigo 5.º do mesmo diploma legal.

18. Considerando agora a captação e gravação das imagens, prevê-se a aplicação de máscaras de privacidade, sempre que as câmaras captem imagens de edifícios destinados à habitação, as quais vêm representadas nas imagens constantes do Anexo B da Fundamentação. E na AIPD esclarece-se que, «[q]uando a mera orientação das câmaras não for suficiente para garantir que áreas privadas não são filmadas, serão criadas zonas de bloqueio digital de gravação através da programação do *software* da própria câmara», especificando-se que, nesses casos, «não haverá visualização em tempo real».

19. 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.

20. Recorda-se ainda 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).

21. 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 de garantia da privacidade, quer no momento da sua definição (pelo instalador), quer quanto ao tipo de credencial necessária para a sua desativação.

iii. A utilização de inteligência artificial para análise de dados pessoais em tempo real – “analítica de dados”

22. Pretende-se ainda, de acordo com a Fundamentação que acompanha o pedido, a análise de imagens com recurso a tecnologia de Inteligência Artificial, tendo o Anexo G como título ou pretensão conteúdo a *«Descrição dos critérios utilizados no sistema de gestão analítica dos dados captados»*.
23. Todavia, o descrito no Anexo G da Fundamentação não corresponde a critérios de análise dos dados pessoais, mas antes à mera descrição das funcionalidades do *software* a utilizar.
24. Aliás, no Anexo G afirma-se, explicitamente, que *«[a]definição de critérios ou padrões de análise é da exclusiva responsabilidade do responsável pelo tratamento e conservação dos dados, não sendo possível aos operadores dos sistemas alterar os padrões criados»*.
25. Sendo certo que a PSP é o responsável pelo tratamento para efeito da Lei n.º 59/2019, de 8 de agosto, e do artigo 17.º da Lei n.º 95/2021 –, é por demais evidente que o pedido de autorização é completamente omissivo quanto aos critérios por que se pauta a utilização desta tecnologia.
26. Apenas se preveem as finalidades da sua utilização, especificando servirem os fins de proteção de pessoas, animais e bens, em locais públicos ou de acesso público, e de prevenção da prática de factos qualificados pela lei como crimes, em locais em que exista razoável risco da sua ocorrência; os fins de controlo de tráfego e segurança de pessoas, animais e bens na circulação rodoviária; e a finalidade de prevenção e repressão de infrações estradais. E acrescenta-se como *«Limite ao sistema de gestão analítica de vídeo»* que *«[n]em o sistema de videovigilância, nem o sistema de analítica de vídeo, permitem a captação e tratamento de dados biométricos conforme determinado no n.º 2 do art. 16º, da Lei 95/2021 de 29 de dezembro»* e que *«[o]s critérios técnicos de análise não podem definir o perfil que conduza a discriminação de pessoas singulares com base nas categorias especiais de dados pessoais, em violação do artigo 6.º da Lei n.º 59/2019, de 8 de agosto»* (cf. Anexo G da Fundamentação). Sendo afirmado na AIPD (cf. p. 16) que o sistema não permite a captação e tratamento de dados biométricos.
27. Importa recordar que 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.
28. 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. Devendo, por isso, ser 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 e pelo órgão com explícita competência consultiva nesta matéria (a CNPD).

29. 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 a 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 descritas no do Anexo G. O que não sucede.

30. Omissa também está a informação relativa ao processamento dos dados: onde ocorre (se em cada uma das câmaras, ou no servidor/*software*), quem gere o processamento, que medidas estão previstas para prevenir a alteração dos critérios, etc.

31. Por outro lado, não é exato dizer-se que o sistema garante que não há tratamento de dados biométricos – como se refere no Anexo G, p. 5, e na AIPD –, pois a circunstância de se declarar que a tecnologia «não tem capacidade de reconhecimento facial» não significa que não haja tratamento de outros dados biométricos.

32. Por outras palavras, as salvaguardas feitas no final do Anexo G, de natureza meramente declarativa ou intencional, são manifestamente insuficientes para assegurar que a operação de análise 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.

33. 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.

34. Deste modo, face à omissão, no pedido, na Fundamentação e na AIPD, da identificação dos critérios subjacentes à utilização do sistema de gestão de análise de dados, a CNPD não consegue verificar se são respeitadas as condições e limites legais e constitucionais a essa utilização, nem o órgão com competência autorizativa tem elementos suficientes para avaliar a proporcionalidade da mesma. A CNPD recomenda, por tudo isto, que esta utilização não seja, por ora, objeto de autorização, sob pena de invalidade da mesma por omissão da consulta imposta pelo n.º 3 do artigo 5.º da Lei n.º 95/2021.

iv. Segurança do sistema de videovigilância

35. Na perspetiva da segurança do sistema de videovigilância, destacam-se aqui os aspetos que não se encontram acautelados e recomendam-se medidas de reforço para integrar algumas insuficiências do sistema.
36. Começando pela instalação física do sistema, não é concretizado como se realizará a instalação física das câmaras e onde ficarão os armários de comunicação. No Anexo D da Fundamentação vem indicado que as câmaras devem *«ter a capacidade de enviar alarme em caso de deteção de ciberataque ou ataque físico»* e ainda as características de proteção da norma utilizada. A CNPD limita-se, por isso, a recomendar que a solução a adotar contemple alarmística de intrusão também nos armários de comunicação onde ficarão ligadas as câmaras, sendo essencial que os mesmos não estejam localizados no chão ou a uma altura que os torne facilmente acessíveis e que, preferencialmente, todos os cabos sejam subterrâneos.
37. Ainda no anexo D vem ilustrada a topologia de conectividade entre câmaras e servidor, podendo ler-se na ilustração que o *switch* local é fornecido pela Câmara Municipal de Olhão.
38. A este propósito, recomenda-se a revisão da topologia de conectividade para seguir boas práticas de segurança, por exemplo, garantindo que apenas o servidor do sistema de videovigilância está na rede das câmaras, com acesso às mesmas, e que o visionamento das imagens nos computadores dos operadores é feito a partir do servidor. Desta forma, todos os acessos serão auditáveis centralmente no sistema, assim como os fluxos de comunicação de dados.
39. Do anexo H da Fundamentação decorre que haverá ecrãs de monitorização no Centro de Controlo de Olhão e também no Centro de Visionamento Principal, localizado no Comando Distrital de Faro. Portanto, o acesso ao sistema será feito em dois pontos geograficamente dispersos. Não vem referida qualquer segregação entre a rede do sistema de videovigilância e as demais, geridas pelo Município e pela própria PSP. Esta partilha de ativos de rede e possibilidade de interligação torna o sistema permeável a tentativas de acesso de terceiros.
40. Assim deve garantir-se a segregação da rede do circuito de videovigilância, e, para que a rede permaneça segregada e isolada, tem de se garantir que os serviços de suporte e manutenção do sistema de videovigilância sejam prestados fisicamente no local, e não remotamente, por causa do risco de exposição do sistema às vulnerabilidades de uma rede aberta.
41. No anexo D da Fundamentação, não estão referidos mecanismos de redundância, alta disponibilidade e resposta ao desastre. Aparentemente não está assegurada a disponibilidade dos dados em relação a avarias no armazenamento, nem está prevista a recuperação dos dados em caso de eliminação accidental. A CNPD sublinha que é essencial contemplar um sistema de cópias de segurança que assegure a disponibilidade dos dados

durante o prazo legal de conservação (30 dias). Na verdade, nada do descrito no anexo D corresponde ou dá resposta ao requisito enunciado no Anexo G: «*A plataforma deverá cumprir requisitos de alta disponibilidade orientados ao suporte de processos críticos, devendo o hardware de suporte da solução estar protegido relativamente a falhas através de mecanismos de redundância. O software de gestão deverá manter o seu funcionamento em caso de falha ao nível do hardware, garantindo a continuidade da operação*».

42. Quanto às câmaras, elas vêm descritas de forma genérica, no anexo D, não sendo indicado o modelo das câmaras, sem que seja possível realizar uma avaliação concreta das suas características. No entanto, as referências à compatibilidade das câmaras com determinado protocolo e ao protocolo em que se baseia a comunicação com a plataforma permitem presumir que as câmaras não enviarão imagens por via analógica e que obedecerão a uma especificada pré-configuração. Assim, é com base nesta premissa que em seguida se enunciam recomendações de segurança.

43. Presumivelmente as câmaras contêm um servidor da *web* integrado para captura de vídeo e configuração disponível num navegador de Internet padrão, usando protocolo HTTP sem necessidade de *software* adicional, protocolo que consabidamente não é cifrado. Esta funcionalidade de administração remota apresenta uma vulnerabilidade de acesso em caso de comprometimento da rede, pois pode haver captura de credenciais de acesso às câmaras, e, se a senha de acesso ao servidor integrado da câmara, que por omissão vem de fábrica, não for trocada, o sistema fica comprometido desde o início. Razões por que o servidor integrado nas câmaras deve ser reconfigurado para HTTPS, deve existir uma política de gestão das senhas nas câmaras e não deve ser utilizada uma senha única para todos os equipamentos.

44. Além disso, não deve expor-se a rede do circuito de videovigilância à conectividade com a Internet, devendo recorrer-se ao uso de VLAN para separar a rede das câmaras das outras comunicações. Finalmente, só devem manter-se abertas, na rede segregada, as portas estritamente necessárias ao funcionamento dos equipamentos.

45. Ainda em relação às medidas de segurança, duas notas: a primeira, para recomendar que os mecanismos de autenticação – de acesso à sala de visualização e de acesso ao sistema – revistam carácter pessoal e intransmissível (v.g., os dois fatores de autenticação devem ser únicos, por cada agente da PSP); a segunda, para sublinhar que a extração de imagens deve ser uma funcionalidade de acesso privilegiado, portanto, não reconhecida a todos os operadores com permissão de visualização das imagens. Deve existir registo de quais as câmaras e intervalo temporal na extração, assim como o responsável pela execução da mesma.

46. Ainda a propósito da extração das imagens, o Anexo H da Fundamentação não explica o processo de extração de imagens, especificamente, como são preservadas estas gravações para serem excecionadas da rotatividade de 30 dias do arquivo do sistema. No âmbito da recolha de imagens, deve ficar 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 ainda prever-se a existência de mecanismos de cifra, caso se pretenda proteger a exportação com uma senha de acesso ou outro fator de segurança. Alguns destes requisitos vêm indicados no Anexo G, a propósito do sistema de gestão analítica de dados, mas, em rigor, estas são exigências a cumprir independentemente da utilização de tal sistema de gestão.

47. Uma última nota, relativa à sincronização com a hora legal, para especificar que é recomendável que o serviço consultado para sincronizar os relógios seja acessível ao servidor de gravação e este atue como serviço de sincronia para as câmaras.

v. Auditabilidade do tratamento de dados pessoais

48. Estando previsto o registo de todas intervenções realizadas ao nível dos sistemas locais, enquanto responsável pelo tratamento de dados pessoais, a CNPD limita-se a reforçar a importância de os serviços de suporte e manutenção ao sistema de videovigilância serem prestados fisicamente no local, sob direta supervisão e acompanhamento pela PSP, enquanto responsável pelo tratamento de dados pessoais, não sendo admissível o acesso remoto na medida em que este pode comprometer a segurança.

49. Para efeito de auditoria do tratamento de dados pessoais, é ainda essencial definir o tempo de conservação dos registos das intervenções e das operações no sistema de videovigilância. Assim, a CNPD recomenda a previsão de uma política de retenção dos registos para efeito de auditoria, definindo-se o período de tempo até ao seu descarte, bem como a previsão dos indicadores chave para os relatórios de auditoria em sede de monitorização da segurança nos acessos e das operações efetuadas.

vi. Subcontratação

50. 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.

51. A CNPD sublinha, a este propósito, que correspondendo, nos termos da lei, o responsável pelo tratamento dos dados *à força ou serviço de segurança requerente [...] com jurisdição na área de captação*, 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 Olhão, podendo esta sub-subcontratar 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.

52. 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.

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

III. Conclusão

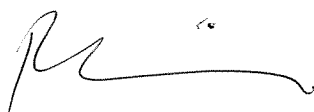
54. Não cabendo na competência que lhe está legalmente atribuída pronunciar-se sobre os concretos fundamentos do alargamento substancial do sistema de videovigilância na cidade de Olhão, a CNPD, com os argumentos acima expostos e ao abrigo da competência conferida pela Lei n.º 95/2021:

- a. Chama a atenção para a imprescindibilidade de clarificação do número de câmaras a instalar, bem como do número total de câmaras que passará a integrar o sistema de videovigilância na cidade de Olhão, em face da incongruência detetada entre o pedido e a documentação que o acompanha;
- b. Recomenda 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;
- c. Destaca que as máscaras de ofuscação para garantia da privacidade devem ser 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 21;
- d. Recomenda ainda a adoção de medidas capazes de garantir a segurança do sistema e a auditabilidade do tratamento de dados pessoais, nos termos assinalados supra, nos pontos 36 a 49;
- e. Recorda a imprescindibilidade de ficar expressa e claramente delimitada em contrato ou acordo a intervenção do Município de Olhão como subcontratante quanto ao tratamento de dados pessoais decorrente da utilização do sistema, bem como de eventuais sub-subcontratantes.

55. Em especial, a CNPD recomenda a não autorização da utilização do 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, pela impossibilidade de verificação do respeito pelas condições e limites legais e constitucionais à sua utilização, em particular, de avaliação da proporcionalidade dessa utilização.

Aprovado na reunião de 15 de novembro de 2022



Filipa Calvão (Presidente)