

## PARECER/2021/125

### 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 utilização de um sistema de videovigilância nas zonas da Oura e Baixa da cidade de Albufeira, submetido pela Guarda Nacional Republicana (GNR).
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).

### 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, 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. As finalidades do tratamento decorrente da Videovigilância em locais públicos de utilização na Oura e na Baixa da cidade de Albufeira**

8. 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).

9. Ora, a utilização de um sistema de videovigilância nas zonas da Oura e Baixa da cidade de Albufeira implica um tratamento de dados pessoais suscetível de afetar significativamente a vida privada das pessoas que aí circulem ou se encontrem.

10. Com efeito, em causa está a instalação e utilização de 64 (sessenta e quatro) câmaras fixas em áreas onde se encontram edifícios destinados à habitação bem como à ocupação por turistas e que são conhecidas por terem grande afluência turística em especial no período balnear (cf. ponto 4.b. da Fundamentação que acompanha o pedido).

11. A este propósito cabe notar que, apesar de o pedido de autorização ser relativo a 64 câmaras, na Fundamentação que o acompanha, encontram-se descritas 65 (sessenta e cinco) câmaras (cf. anexo A da referida Fundamentação). Desconhecendo a CNPD se esta discrepância se deve a um lapso ou se há alguma câmara que não se pretende ver abrangida em eventual autorização a emitir, limita-se esta entidade a assinalar tal facto, chamando a atenção para a circunstância de que, na falta de especificação da câmara a excluir, a licitude do tratamento de dados pessoais realizado com base nas imagens captadas por qualquer das câmaras fica em risco.

12. Acresce que a maior parte das câmaras 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. Entre as que não têm PTZ, algumas parecem ter pelo menos a funcionalidade de *Pan* (rotação).

13. 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, bem como a finalidade de prevenção de atos terroristas, nos termos das alíneas c) e e) do n.º 1 do artigo 2.º da Lei n.º 1/2005.

14. Para o efeito, declara-se que o sistema de videovigilância procede *unicamente* à captação e gravação de imagens, mas, apesar de não se pretender a gravação de som, prevê-se ainda a *instalação e uso do mecanismo de funcionamento do sistema denominado «alerta de voz»* (cf. ponto 4.c. da Fundamentação).

15. E ainda se declara que *«[e]m caso de necessidade poderá se[r] utilizada analítica de vídeo, no entanto estão definidas regras integradas diretamente na câmara (Anexo B), no sentido de inviabilizar qualquer criação de perfis ou d[i]scriminação de pessoas, conforme previsto no artigo 6.º da Lei n.º 59/2019, de 8 de agosto»* (cf. ponto 4.g. da Fundamentação). A este ponto voltar-se-á, mas para a apreciação do respeito pelas condições e limites impostos no artigo 7.º da Lei n.º 1/2005, no âmbito da competência consultiva da CNPD, desde já se adianta não estarem definidas quaisquer *regras* no Anexo B, mas meramente *funcionalidades ou potencialidades da câmara*. Por essa razão, a utilização de analítica de vídeo por recurso a tecnologia de Inteligência Artificial, de *soft recognition*, sem especificação dos termos em que a mesma vai ter lugar, permite ou promove o rastreamento de qualquer cidadão sem garantias de não discriminação e sem garantias de proporcionalidade na compressão do direito fundamental à reserva da vida privada que a todos é reconhecido, inclusive no contexto da circulação em espaço público (cf. artigo 26.º da Constituição da República Portuguesa – CRP).

16. Mesmo sem considerar, por ora, a aplicação da referida tecnologia, o impacto na privacidade dos cidadãos da utilização deste sistema de videovigilância é manifestamente elevado, não apenas tendo em conta o âmbito e extensão das áreas sobre que incidem as câmaras que captam e gravam imagens (cf. supra ponto 10), mas também por força da aparente potencialidade de captação de som, que um mecanismo de «alerta de voz» à partida comporta e cujos termos e condições de execução não vêm em ponto algum do pedido ou da Fundamentação descritos – ainda que no ponto 1.a) do Anexo B e da AIPD se afirme, respetivamente, que *«as câmaras não permitem que seja capturado qualquer tipo de som»* e *«o sistema não permite tecnicamente a captação e gravação de som»*

17. Na verdade, apesar de se prever a *instalação e uso do mecanismo de funcionamento do sistema denominado «alerta de voz»*, em lado algum se explicita em que consiste tal mecanismo e, portanto, fica por esclarecer se o alerta é acionado através da captação de som pelas câmaras ou se opera por via de altifalante que permita à GNR lançar alertas para quem se encontre nas proximidades das câmaras. Mesmo que o que esteja em causa seja a segunda hipótese aqui considerada, o sistema pode permitir que ao ser ativado o altifalante seja também captado som, caso em que é indispensável assegurar a desativação da funcionalidade de captação de som. Repare-se que, não havendo lugar à captação e gravação de som a partir das câmaras de videovigilância, o



requisito para a estação de trabalho de monitorização de *«possuir alto-falante interno que seja desativado automaticamente quando conectado algum dispositivo de áudio externo a interface de som "line-out" frontal, transferindo a reprodução do som para esse dispositivo»*, patente no ponto 3. do anexo B, evidencia que se pretende contemplar a escuta de áudio de alguma natureza.

18. Insiste-se que a captação de som, nas imediações de casas de habitação e de edifícios hoteleiros ou de alojamento local, mas também em espaços públicos, impacta de sobremaneira na privacidade, não devendo ocorrer salvo se se demonstrar a sua imprescindibilidade para a finalidade visada com este tratamento de dados e estejam estabelecidas as condições objetivas em que a mesma ocorre.

19. Acresce que, embora se preveja a adoção de medidas destinadas a salvaguardar a privacidade das pessoas dentro dos edifícios e de espaços privados – *«colocação de máscaras nas câmaras de modo a não captarem e não gravarem imagens em locais privados, como o interior de habitações ou quintais»* (cf. ponto 4.c. da Fundamentação) –, a verdade é que os elementos apresentados não permitem aferir do respeito pelos limites impostos no n.º 6 do artigo 7.º da Lei n.º 1/2005. Com efeito, no Anexo A são apresentados os ângulos prováveis de visão das câmaras, e apesar de se referir logo no parágrafo inicial *«um sistema configurável para ocultar áreas definidas da imagem, tornando-as não exibíveis, tais como janelas ou entradas de edifícios, como no seu interior. Essas máscaras serão inclusive dinamicamente ajustadas com base no fator de zoom atual e o operador não consegue exibir os conteúdos protegidos»*, nas imagens que se seguem não são assinaladas as zonas a filtrar ou ocultar, nem as mesmas indiciam um trabalho de identificação das exatas câmaras que incidem sobre essas zonas.

20. Assim, com os fundamentos supra expostos, a CNPD entende não existir informação suficiente no pedido e nos documentos apresentados que permitam à CNPD, tão-pouco ao órgão competente para a autorização da utilização do sistema, avaliar do respeito pelos limites impostos no n.º 6 do artigo 7.º da Lei n.º 1/2005.

21. Quanto à captação de som, se se confirmar que as câmaras comportam tal funcionalidade, a CNPD recomenda que, a ser autorizada, seja na referida autorização enquadrada por orientações precisas, não podendo ficar dependente de critérios subjetivos do agente que no momento esteja a operar o sistema.

### iii. Aptidão do sistema de videovigilância para rastreamento dos cidadãos

22. Como se referiu supra, no ponto 15, no pedido afirma-se que *«[e]m caso de necessidade poderá se[r] utilizada analítica de vídeo, no entanto estão definidas regras integradas diretamente na câmara (Anexo B), no sentido de inviabilizar qualquer criação de perfis ou d[is]criminação de pessoas, conforme previsto no artigo 6.º da Lei n.º 59/2019, de 8 de agosto»* (cf. ponto 4.g. da Fundamentação).

23. Esclarece-se que, de acordo com as características das câmaras descritas no ponto 1.a) do referido Anexo B, tal significa a aptidão do sistema de videovigilância para identificar cidadãos a partir de características físicas e o rastreamento dos mesmos, inclusive para acompanhar os seus comportamentos e hábitos. Na verdade, apesar de se declarar no ponto 5 do Anexo B que *«[o] sistema não recolhe metadados para identificações, pelo que não identifica pessoas nem viaturas, só aparências»*, a própria finalidade do sistema de videovigilância e da tecnologia de *soft recognition* não pode ser outra que não a identificação das pessoas e o reconhecimento dos objetos. Eventualmente, com aquela afirmação, pretender-se-á invocar que não se faz reconhecimento facial, como noutro ponto reafirmam, mas tal não significa que a não identificabilidade das pessoas captadas nas imagens e seu rastreamento automatizado.

24. Ora, a utilização desta tecnologia, sobretudo num ambiente de controlo sistemático e em larga escala de zonas acessíveis ao público, tem de ser precedida de uma cuidadosa ponderação das consequências da mesma, não apenas para privacidade das pessoas, como também para as dimensões fundamentais de liberdade, identidade pessoal e de não discriminação. É, pois, essencial que estejam predefinidas as circunstâncias da sua utilização – ou seja a caracterização das situações que podem revelar a *necessidade* da sua utilização tendo em vista as finalidades do tratamento de dados – para que se possa avaliar da proporcionalidade das restrições àqueles direitos fundamentais, consagrados nos artigos 13.º e 26.º da CRP, nos termos impostos pelo n.º 2 do artigo 266.º da Lei fundamental.

25. E, para esse efeito, essencial seria também que a AIPD realizada tivesse incidido especificamente sobre este tratamento de dados pessoais. Todavia, na AIPD refere-se somente que *«o sistema tem capacidade de adicionar análíticas de vídeo para proteger pessoas e bens, com regras de deteção»* e conclui-se estarem *«salvaguardadas as garantias suficientes»* para os direitos, liberdades e garantias.

26. Simplesmente, no ponto 1.a) do Anexo B, além da referência expressa de que as câmaras não permitem o reconhecimento facial, apenas se elencam as potencialidades ou funcionalidades das câmaras de videovigilância que as mesmas integram, em ponto algum se definindo os critérios e os limites da sua utilização. Na verdade, do declarado resulta que o sistema permite selecionar e acompanhar um determinado «objeto», que pode ser uma pessoa ou um veículo, explicitando-se que *«o evento é disparado quando o tipo de objeto selecionado se move para a região de interesse» «permanece dentro da região de interesse por um período prolongado», «para de se mover por um limite de tempo especificado», etc.*, sem se explicitar os critérios de seleção do «objeto» de análise, tão-pouco da «região de interesse».

27. Por outras palavras, o pedido e a fundamentação que o acompanha são omissos quanto às situações que justificam a utilização do algoritmo de análise das imagens, bem como quanto aos critérios ou fatores que

podem estar na base da seleção das pessoas ou veículos para rastreamento. E a definição dos pressupostos da sua utilização e destes critérios ou fatores de seleção tem de ser feita previamente em termos que previnam o risco de discriminação em função de certas características ou perfis, no respeito pelas condições e limites fixados no artigo 13.º da CRP e no n.º 1 do artigo 9.º do RGPD, porventura com imposição de que sejam definidos *ex ante* fatores ou critérios de análise não admissíveis.

28. Estes pressupostos e fatores, na falta de lei que os elenque e densifique, têm de estar definidos em eventual autorização a emitir, sob pena de não se conseguir perceber se os resultados apresentados pelo sistema, e com base nos quais a GNR vai tomar decisões sobre os cidadãos visados, são discriminatórios e, portanto, inadmissíveis à luz da Constituição.

29. Face à omissão de tais elementos no pedido e na fundamentação, a CNPD recomenda que eventual decisão autorizativa sobre a instalação e utilização deste sistema de videovigilância não cubra a utilização desta tecnologia de analítica de vídeo, proibindo-se expressamente a ativação das funcionalidades de Inteligência Artificial que permitem o rastreamento automatizado dos cidadãos ou de veículos.

#### iv. Subcontratação

30. Em relação à utilização 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.

31. 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 GNR. Não está afastada a hipótese de a GNR subcontratar o Município de Albufeira, 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 GNR sem o domínio ou controlo do tratamento de dados pessoais que o sistema de videovigilância realiza.

32. Sendo certo que no ponto 5. da Fundamentação, se afirma que a GNR será a única entidade a deter o controlo das câmaras, importa, por isso mesmo, que seja celebrado um contrato ou acordo a regular 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.

33. 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**

34. Há aspetos descritos na Fundamentação que suscitam reservas à CNPD quanto à segurança do sistema de videovigilância, desde logo no que diz respeito à arquitetura das comunicações.

35. Começa-se por considerar a referência, no ponto 1.a) do anexo B, a propósito das características das câmaras de videovigilância, de que as mesmas «*contêm um servidor web integrado para captura de vídeo e configuração disponível num navegador da Internet padrão, usando HTTP sem necessidade de software adicional*».

36. Esta funcionalidade apresenta uma vulnerabilidade de acesso em caso de comprometimento da rede pois pode haver captura de credenciais de acesso às câmaras, sendo certo que o protocolo HTTP não é cifrado. Também se coloca em questão a credencial de acesso ao servidor integrado da câmara. Caso não seja trocada a senha por omissão que vem de fábrica, o sistema fica comprometido desde o início

37. Assim, recomenda-se que o servidor integrado nas câmaras seja reconfigurado para HTTPS e que se preveja uma política de gestão das senhas nas câmaras, não devendo ser utilizada uma senha única para todos os equipamentos.

38. Aliás, refere-se na Fundamentação que a encriptação de todas as imagens, entre a câmara e o servidor de gravação, mas, apesar de se referir no ponto 1.a) do Anexo B a criptografia HTTPS, no mesmo ponto se afirma que as câmaras são compatíveis com outros protocolos. A CNPD, além de sublinhar que aquele protocolo de cifra apenas é seguro se implementado na versão TLS1.2 ou superior, recomenda que todos os protocolos que não sejam essenciais ao funcionamento do sistema de videovigilância devem ser desativados.

39. Maior apreensão suscita a interligação deste sistema de videovigilância com a RNSI (Rede Nacional de Segurança Interna).

40. Na verdade, de acordo com o declarado na Fundamentação, as imagens serão transmitidas para dois locais distintos, para efeito de monitorização: o Destacamento Territorial de Albufeira e a Sala de Situação do Comando Territorial de Faro.

41. Além de não estar claro como se articulam as duas salas de monitorização (por exemplo, pressupondo que o sistema tem apenas uma matriz de vídeo (*video wall*)), conviria esclarecer se as alterações na sua visualização



afetam os dois postos de controlo e qual a articulação pensada entre eles), há questões que se levantam a propósito da ligação entre a rede de comunicações do sistema de videovigilância e a RNSI. Vejamos.

42. Por um lado, no ponto 4.g. da Fundamentação refere-se que «[a] transmissão das imagens para a Sala de Situação do Comando Territorial de Faro será através da Rede Nacional de Segurança Interna (RNSI) com todas as políticas de segurança nas comunicações inerentes a esta rede» e que a entrada nas salas destinadas à visualização de imagens é reservada «aos militares credenciados para o efeito, sendo registadas e controladas, mediante a introdução de um código de entrada e o acesso ao sistema de visualização mediante a atribuição de perfis de acesso RNSI». O que é confirmado na AIPD (cf. anexo D), onde se menciona que «o acesso ao sistema de visualização só é possível através da atribuição de perfis de acesso RNSI» e que «a transferência das imagens para a Sala de Situação do Comando Territorial de Faro é realizada através da RNSI».

43. Por outro lado, de acordo com o protocolo celebrado entre a GNR e o Município de Albufeira, a instalação e gestão da rede de comunicações que ligará as câmaras de videovigilância à sala de controlo e ao servidor de gravação ficará a cargo do Município de Albufeira – o que só pode suceder em regime de subcontratação, como se assinalou supra, pontos 30 a 32.

44. Estes factos indicam que haverá uma interligação entre a RNSI e a rede de videovigilância, esta última, de facto, gerida pelo Município, sobre a qual, contudo, nada se diz na Fundamentação.

45. Ora, se a rede de comunicações do Município de Albufeira for uma rede privada, como os trabalhadores do Município têm acesso à rede da autarquia, há risco de qualquer um deles (desde que esteja certificado na rede do Município) aceder às câmaras de videovigilância, adquirindo facilmente o domínio sobre as mesmas (o que lhes permite, por exemplo, fazer zoom, retirar máscaras ou filtros, ligar ou desligar as câmaras, substituir as imagens por outras, etc.). Mas se a rede do Município for uma rede pública aberta (simplificando a linguagem, uma rede de Internet HTTP), há ainda o risco de qualquer pessoa aceder às câmaras e conseguir o domínio sobre elas.

46. Mais grave ainda é que as vulnerabilidades da rede do Município se estendem à RNSI, por força da interligação entre as duas redes. Na realidade, uma eventual intrusão ou propagação de *software* maldoso na rede do município, poderá propagar-se à RNSI. Por outro lado, apesar de se declarar que estão salvaguardadas todas as políticas de segurança nas comunicações inerentes à RNSI, as mesmas poderão não se aplicar a uma rede com gestão de uma terceira entidade, no caso um município.

47. A CNPD recomenda, por isso, que na autorização se imponha a segregação física e lógica das redes de videovigilância das outras redes, com aplicação de protocolo HTTPS. E chama a atenção para o facto de, a menos que seja demonstrado que a rede das câmaras de videovigilância e o servidor de gravação são



fisicamente dedicados e segregados de outros ativos de rede municipais e que a gestão dessa rede pelo Município se rege pelas mesmas políticas de segurança inerentes à RNSI, o cenário de interligação proposto é de risco elevado.

48. Uma outra característica do sistema de videovigilância que suscita a maior apreensão prende-se com a referência à consola de gestão que permite a *«visualização remota a partir de qualquer dispositivo»* – cf. ponto 5. do Anexo B. Na perspetiva da segurança do sistema o acesso remoto implica um risco muito elevado, devendo estar, por isso, vedada tal possibilidade. 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 acessos ao sistema de videovigilância sejam fisicamente na sala de controlo, não sendo admissível o acesso remoto na medida em que este pode comprometer a segurança.

49. Focando agora a segurança física do sistema de videovigilância, destaca-se que não é concretizado como se realizará a instalação física das câmaras, nem onde ficarão instalados os armários de comunicação.

50. Quanto às câmaras de videovigilância, no ponto 1.a) do Anexo B especifica-se que têm *«características anti vandálica com parafusos resistentes à adulteração»*. Mas não é referido um mecanismo de “anti-tampering” nos armários, com alertas. É certo que, no mesmo Anexo, ponto 5., se indica que *«[a] plataforma de software tem um “Site health” para a GNR saber a todo o momento os estados de todos os equipamentos que estão a interagir com a plataforma»*. Afigurando-se que por equipamento se pretende referir as câmaras e não os ativos de comunicação, se uma câmara estiver operacional, mas o seu bastidor de comunicação for comprometido, não parece estar assegurado um alerta no sistema.

51. Assim, a CNPD recomenda que a solução a adotar contemple alarmística de intrusão também nos armários de comunicação onde ficarão ligadas as câmaras. Demais, tendo em conta o 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 essencial que os armários de comunicações (instalados no espaço público) não estejam localizados no chão ou a uma altura que os torne facilmente acessíveis.

52. Considerando que, no mesmo Anexo B, se declara que as câmaras, do ponto de vista de conectividade em rede, possuem apenas *«uma porta Gigabit Ethernet 1 000BASE-TX, usando um soquete RJ-45 padrão»*, conclui-se que, de acordo com a arquitetura definida, cada câmara se ligará ao armário de comunicação por cabo UTP. Neste pressuposto, é essencial que esse cabo não fique exposto, sendo idealmente subterrâneo.

53. Importa ainda considerar as condições relativas à recuperação dos dados, em caso de eliminação accidental. Refere-se no ponto 2.1. do anexo B que o armazenamento de dados *«[p]ossui uma controladora RAID*

*dedicada com memória RAM de 32GB DDR ou superior, suportando varies níveis de RAID. As configurações da controladora RAID são replicadas nos discos rígidos permitindo desta forma maior tolerância a falhas». Está, pois, assegurada a disponibilidade dos dados em relação a avarias no armazenamento, mas não está prevista a recuperação dos dados em caso de eliminação accidental. Assim, recomenda-se que seja contemplado um sistema de cópias de segurança que assegure a disponibilidade dos dados dentro da janela temporal definida que são os 30 dias.*

54. Consta ainda do ponto 5 do Anexo B a «*[m]aior confiabilidade com alta tolerância as falhas sendo previsto failover para este sistema*». O cenário de *failover*, apesar de referido, não está documentado. A este propósito assinala-se que, para poder existir este cenário, é preciso que estejam quantificados, não apenas um, mas dois servidores, com a arquitetura de partilha da unidade dedicada de armazenamento de dados. Só desta forma se assegura a continuidade do sistema em caso de falha no servidor ativo, passando a funcionar no servidor passivo.

55. Finalmente, importa densificar o controlo de entradas e saídas das salas onde decorrem os tratamentos de dados pessoais. No ponto 4.g. da Fundamentação e na AIPD descreve-se o sistema de controlo de entradas nas diferentes salas, mas importa que o mecanismo de controlo – para ser plenamente apto a identificar quem, em cada momento, se encontra nas duas salas – registe, além das entradas, também as saídas. Só desse modo, é possível demonstrar a imputabilidade subjetiva de qualquer evento.

56. Finalmente, assinala-se que não há informações suficientes sobre o procedimento de extração de imagens para efeito de investigação criminal. Em especial, recomenda-se a definição de regras sobre o procedimento de preservação das imagens extraídas, incluindo como são preservadas estas gravações para serem excecionadas da rotatividade de 30 dias do arquivo do sistema, e que garantam a sua eliminação após a conclusão do processo-crime.

57. 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 aludir à presença de mecanismos de cifra, caso se pretenda proteger a exportação com uma senha de acesso ou outro fator de segurança

#### **vi. Auditabilidade do tratamento de dados pessoais**

58. Quanto à previsão da existência de *logs* (registos cronológicos), no ponto 5. da Fundamentação, 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.

59. 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*.

60. 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.

61. 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, recordando-se que a função dos registos cronológicos só é atingida se os mesmos forem objeto de análise.

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

### III. Conclusão

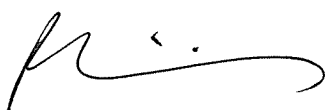
63. Não cabendo na competência que lhe está legalmente atribuída pronunciar-se sobre os concretos fundamentos da utilização do sistema de videovigilância nas zonas da Oura e Baixa da cidade de Albufeira, a CNPD, com os argumentos acima expostos:

- a. Entende não haver elementos que permitam avaliar se o sistema não impacta de forma desproporcionada sobre a privacidade e intimidade das pessoas que se encontram dentro dos edifícios ou espaços privados, máxime destinados a habitação e a hotelaria, não podendo assim atestar se são respeitados os limites fixados no n.º 6 do artigo 7.º da Lei n.º 1/2005;
- b. Recomenda que seja densificada a regulação do mecanismo de «alerta de voz», nos termos explicitados supra, nos pontos 16, 17 e 21;
- c. Insiste que, sendo o responsável pelo tratamento de dados pessoais, nos termos da lei, a GNR, tem de ficar expressa e claramente delimitada em contrato ou acordo a intervenção do Município de Albufeira como subcontratante desta entidade, e de eventuais subsubcontratantes;

d. Uma vez que o *software* aplicado compreende funcionalidades de Inteligência Artificial que permitem o rastreamento dos cidadãos, não estando à partida definidos os pressupostos e os critérios da sua utilização, recomenda que em eventual decisão autorizativa sobre a utilização deste sistema de videovigilância seja proibida expressamente a ativação dessas funcionalidades.

64. 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, em especial nos pontos 37, 38, 47, 48, 51, 52 a 58 e 61.

Lisboa, 20 de setembro de 2021



Filipa Calvão (Presidente, que relatou)