

PARECER/2019/92

I. Pedido

1. Em 4 de outubro de 2019, por despacho da Secretária de Estado Adjunta e da Administração Interna, foi solicitado parecer à Comissão Nacional de Proteção de Dados (CNPD) sobre o pedido de autorização de instalação de um sistema de videovigilância na cidade de Portimão, submetido pela Polícia de Segurança Pública (PSP).

Tendo entretanto sido reiterado o interesse na emissão do presente parecer no âmbito do procedimento autorizativo da competência do membro do Governo que tutela a força ou serviço de segurança requerente, a CNPD aprecia o projeto nos termos e para os efeitos da Lei n.º 1/2005, de 10 de janeiro, alterada e republicada pela Lei n.º 9/2012, de 23 de fevereiro, que regula a utilização de sistemas de vigilância por 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.

O pedido vem acompanhado de um documento do qual consta a fundamentação do pedido e a informação técnica do sistema, doravante designado por “Fundamentação”.

II. APRECIÇÃO

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

Nos termos do n.º 2 do artigo 3.º da Lei n.º 1/2005, de 10 de janeiro, na redação dada pela Lei n.º 9/2012, de 23 de fevereiro (doravante, 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.

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.

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.

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.

2. Videovigilância em locais públicos de utilização comum na cidade de Portimão para a finalidade de proteção de pessoas e bens e prevenção de crimes

2.1. Ponto prévio

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 para a finalidade de proteção de pessoas e bens, 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 abranja interior de casa ou edifício habitado ou sua dependência ou afete, de forma direta e imediata, a intimidade das pessoas, ou resulte na gravação de conversas de natureza privada (cf. n.ºs 4, 6 e 7 do artigo 7.º da Lei n.º 1/2005).

Ora, a instalação de um sistema de videovigilância na cidade de Portimão implica um tratamento de dados pessoais que, pelo seu âmbito e extensão, parece afetar significativamente a vida privada das pessoas que circulem ou se encontrem naquela cidade. Na verdade, como melhor se desenvolverá infra, são vários os aspetos e as características deste sistema que justificam a apreensão da CNPD quanto a um especial

impacto deste tratamento de dados pessoais sobre os direitos fundamentais dos respetivos titulares. Vejamos.

Em primeiro lugar, pretende-se instalar um sistema de videovigilância na cidade de Portimão, num total de sessenta e uma câmaras. Cinquenta e uma câmaras estarão localizadas em três zonas da Praia da Rocha (zona poente, zona central e zona nascente), «*a fim de garantir a proteção e segurança de pessoas e bens, e da atividade económica da zona de abrangência deste sistema de videovigilância no Município de Portimão, contra atos de vandalismo e ilícitos criminais*». As restantes dez câmaras fixas «*nos principais eixos rodoviários de acesso à cidade de Portimão com a finalidade principal de prevenção e repressão de infrações estradais*» (cf. Anexo A da Fundamentação, bem como Anexo D).

Para além de ser óbvio que o sistema de videovigilância em locais públicos de utilização comum não pode, nos termos da Lei n.º 1/2005, servir para prevenção ou repressão de «atos de vandalismo», tão-pouco para combater «incividades» (como se invoca nos fundamentos do pedido e também no anexo A da Fundamentação), e de os demais fundamentos apresentados não traduzirem qualquer ponderação, à luz do princípio da proporcionalidade, que não seja a consideração da eficácia (e alegado menor custo) do desempenho da função de prevenção e repressão criminais, sem atender ao impacto que da utilização de tal sistema resulta ou pode resultar para os direitos fundamentais dos cidadãos, os termos em que vem apresentado o pedido de instalação do sistema permite compreender que a privacidade das pessoas e outras suas dimensões fundamentais vão ser significativamente afetadas.

Por um lado, a acrescer ao alargado âmbito de incidência das câmaras (praticamente toda a Praia da Rocha), deve considerar-se que tais 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 e veículos, numa área destinada a lazer e onde, durante o dia, as pessoas se encontram mais expostas, pelo que maiores cautelas se impõem na utilização deste tipo de sistemas. Por outro lado, há ainda que considerar que está prevista e é solicitada autorização para captação de som, com evidente impacto na privacidade.

Mas sobretudo, destaca-se a circunstância de o sistema de videovigilância apresentar como características a «*Utilização de tecnologias (hardware e software) no estado de*



arte, incluindo análise inteligente de vídeo no software [...]»; «a capacidade [de] tratar automaticamente eventos não usuais e apresentá-los em vídeo gravado simplificada ao operador»; «Possuir procura avançada por descrições físicas tais como cores das roupas (parte de baixo e parte de cima), sexo (M/F), cor de cabelo [...]»; «Possibilidade de, no futuro, ter capacidade de leitura de matrículas (LPR)»; «A plataforma de software deverá ter analítica de vídeo de "movimentos de deteção anormais" do mesmo fabricante» (cf. Anexo B da Fundamentação).

Em causa está a utilização de tecnologia de Inteligência Artificial (IA) e de *soft recognition*, a qual poderá afigurar-se idónea, em determinadas circunstâncias, para as finalidades visadas. É o caso da funcionalidade de leitura de matrículas que pode agilizar a prossecução de finalidades elencadas no artigo 13.º da Lei n.º 1/2005. Mesmo para a prevenção e repressão criminal no domínio da proteção de pessoas e bens, não se questiona a adequação da sua utilização.

Todavia, e começando pela tecnologia de *soft recognition*, não se alcança como se pode, por via da inserção no sistema de características físicas de pessoas ou de matrículas de veículos, garantir uma melhor gestão de tráfego ou mesmo a prevenção de acidentes ou prestação mais eficiente de socorro em caso de acidente rodoviário. Mas, mesmo para a prossecução da finalidade de proteção de pessoas e bens, a utilização de tecnologia que permite o rastreamento da deslocação e dos comportamentos das pessoas carece de uma específica demonstração da necessidade da sua utilização, o que no caso concreto não sucede.

Na verdade, em ponto nenhum da fundamentação se explica a necessidade dessa concreta tecnologia e funcionalidade, para cada um dos dois grupos de câmaras, os quais prosseguem finalidades bem distintas, que não justificam evidentemente medidas restritivas da privacidade de igual intensidade.

Neste contexto diversificado de utilização de sistema de videovigilância, com o âmbito e incidência das sessenta e uma câmaras, compete à CNPD destacar a necessidade de ponderação da utilização destes tipos de tecnologia, considerando o impacto que da mesma pode decorrer para as pessoas abrangidas pelo raio de captação das câmaras.

Não se trata, pois, de uma rejeição absoluta da utilização pelas forças de segurança da tecnologia que hoje a ciência e o mercado disponibilizam. Apenas se pretende que a utilização dos sistemas de videovigilância e, em particular, da tecnologia de *soft*

recognition seja precedida de uma cuidadosa ponderação das consequências da mesma para a privacidade das pessoas, bem como para outras dimensões fundamentais do ser humano diretamente postas em crise com este tipo de tratamentos de dados pessoais, como seja a liberdade e o direito à igualdade (aqui em crise, uma vez que o risco de rastreabilidade de comportamentos e hábitos, bem como a seleção de características físicas para a *soft recognition*, pode gerar o condicionamento da liberdade de ação e controlos discriminatórios a partir de determinados perfis).

Do mesmo modo, e até por um argumento de maioria de razão, a utilização de IA tem de ser precedida de ponderação especialmente rigorosa. Com efeito, analítica de vídeo funciona através de um algoritmo que é programado para responder a estímulos e movimentos específicos, matéria sobre a qual a Fundamentação é completamente omissa. Na verdade, em ponto algum da Fundamentação se esclarece qual o algoritmo a utilizar, de que pressupostos o mesmo partirá e quais as respostas (*outputs*) que se pretendem atingir.

Note-se que o que agora aqui se apresenta é uma solução de IA e visão computacional. Nessa medida, a sua utilização tem, obviamente, de ser devidamente enquadrada com pressupostos e critérios pré-definidos (porventura com programação de critérios de análise de informação não admissíveis, em face do regime jurídico vigente), sob pena de não se conseguir perceber se os resultados apresentados pelo sistema, e com base nos quais a PSP vai tomar decisões sobre os cidadãos visados, são discriminatórios e, portanto, inadmissíveis à luz da Constituição da República Portuguesa.

É, pois, evidente que a utilização de IA, em especial quando utilizada 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 a liberdade, a identidade pessoal e o direito à não discriminação.

Ora, estas ponderações podem e devem ser feitas pelo legislador, numa desejável regulação destas tecnologias, uma vez que o regime contido na Lei n.º 1/2005, apesar da revisão de 2012, não parece ter tomado em conta a evolução tecnológica entretanto ocorrida, mas sobretudo tem de ser feita no âmbito do procedimento autorizativo da instalação e funcionamento de concretos sistemas de videovigilância, como o que aqui está em causa.

O juízo de ponderação pauta-se, evidentemente, pelo princípio da proporcionalidade, não apenas quanto à utilização do sistema de videovigilância com esta extensão e incidência na cidade de Portimão, mas também especificamente quanto às tecnologias de *soft recognition* e de IA, para que se avalie da sua adequação e necessidade (e proporcionalidade) à prossecução das finalidades visadas com essa utilização, e se conclua se há ou não uma efetiva correspondência entre as vantagens ou potencialidades da utilização daquele sistema e daquela tecnologia e a proteção dos dados pessoais e demais direitos fundamentais associados.

Desenvolvendo, há que avaliar, primeiro em relação ao sistema de videovigilância com as 61 câmaras, depois especificamente em relação às tecnologias de *soft recognition* e de IA, que tipo de crimes ou infrações justificam a sua utilização e em que medida se revelam adequadas a prevenir ou reprimir esses ilícitos, se essa adequação e necessidade se manifesta em todas as áreas territoriais do concelho cobertas pelo sistema ou se apenas em algumas zonas mais delimitadas, etc. Tendo ainda especialmente em conta que a afetação do direito fundamental ao respeito pela vida privada é irreversível, não sendo suscetível de reintegração.

Aliás, a nova Lei n.º 59/2019, de 8 de agosto, que aprova as regras relativas ao tratamento de dados pessoais para efeitos de prevenção, deteção, investigação ou repressão de infrações penais ou de execução de sanções penais, transpondo a Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, impõe ao responsável por estes tratamentos de dados pessoais a realização de uma avaliação de impacto sobre a proteção de dados quando deles decorram *risco elevado para os direitos, liberdades e garantias das pessoas*.

Importa, a este propósito, recordar que o n.º 2 do artigo 2.º da Lei n.º 1/2005 determina que o tratamento de dados pessoais decorrente da utilização do sistema de videovigilância se rege pelo disposto na Lei n.º 67/98, de 26 de outubro, em tudo o que não seja especificamente previsto na presente lei, e que esta lei, quanto aos tratamentos realizados para efeitos de prevenção, deteção, investigação ou repressão de infrações penais ou de execução de sanções penais, foi revogada e substituída pela Lei n.º 59/2009, de 8 de agosto. Considerando ainda que, no n.º 3 do artigo 67.º deste último diploma legislativo se determina que «*Todas as referências feitas à Lei da Proteção de Dados Pessoais, aprovada pela Lei n.º 67/98, de 26 de outubro, consideram -se feitas para o regime da presente lei, quando disserem respeito à proteção das pessoas*

singulares relativamente ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, deteção, investigação ou repressão de infrações penais ou de execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública», só pode concluir-se pela aplicação direta do disposto no artigo 29.º aos tratamentos de dados pessoais decorrentes da utilização de sistemas de videovigilância.

Assim, tendo em conta que este tratamento implica um controlo sistemático em larga escala na cidade de Portimão e que o mesmo promove o rastreamento das pessoas e dos seus comportamentos e hábitos, bem como a identificação das pessoas a partir de dados relativos a características físicas, é inegável o risco elevado que o mesmo importa para os direitos, liberdades e garantias das pessoas, em especial dos direitos fundamentais à proteção dos dados e ao respeito pela vida privada, bem como à liberdade de ação e ao direito à não discriminação.

Por tudo isto, a CNPD considera que o artigo 29.º da Lei n.º 59/2019, de 8 de agosto, é aplicável no procedimento autorizativo em curso, recomendando-se, por isso, uma análise cuidada dos riscos para os direitos das pessoas e a avaliação criteriosa das medidas previstas para os mitigar. Aliás, tendo em conta que a utilização de uma parte das câmaras visa a prevenção e repressão de infrações estradais (quanto não correspondam a um ilícito criminal) e a gestão de tráfego, a avaliação de impacto sobre a proteção de dados sempre seria obrigatória nos termos do n.º 1 e da alínea c) do n.º 3 do artigo 35.º do Regulamento (UE) 2016/679, de 27 de abril de 2016 (RGPD).

Em particular, deve nessa avaliação considerar-se autonomamente cada uma das finalidades visadas e atentar-se nos aspetos do tratamento que a análise das características técnicas do equipamento e demais elementos constantes da Fundamentação permite por ora destacar e que a seguir se enunciam.

Deve ainda aplicar-se os princípios e regras de proteção de dados desde a conceção e por defeito, nos termos impostos pelo artigo 21.º da Lei n.º 59/2019, de 8 de agosto, e pelo artigo 25.º do RGPD.

2.2. Das características técnicas do sistema

Antes de se iniciar a apreciação das características técnicas do sistema, importa notar que o pedido de autorização de instalação do sistema de videovigilância não descreve,

em rigor, as características dos sistemas sobre os quais será realizado o tratamento, mas sim, as características técnicas que a PSP determinou que seriam exigíveis para esses equipamentos¹. Os dois conceitos diferem, uma vez que o primeiro caracteriza a forma como foi implementada uma tecnologia, enquanto o segundo pode compreender múltiplas tecnologias diferentes e também múltiplos cenários de implementação diferentes. É, portanto, a diferença entre aquilo que “é” e aquilo que “pode ser” que dificulta a avaliação da CNPD quanto à conformidade do sistema com as condições e limites fixados no n.º 2 do artigo 3.º da Lei n.º 1/2015 e na Portaria n.º 372/2012, de 16 de novembro.

Demais, há aspetos do tratamento de dados realizado por ou com base no sistema de videovigilância que vêm indiciados na descrição das características técnicas, mas em relação aos quais não há informação que permita compreender os seus contornos e os seus fundamentos.

É o caso da referência, tanto no Anexo A como no Anexo B, à funcionalidade de «*leitura de matrículas (LPR) de viaturas*». Ora, uma vez que não é referida qualquer interconexão, seja automática seja por consulta manual, com sistemas de registo de veículos motorizados ou outras bases de dados, não se entende como se pretende atingir a finalidade de deteção de matrículas falsificadas e veículos furtados, referida na Fundamentação. Assim, a CNPD não tem elementos para se pronunciar sobre esta eventual operação de dados pessoais autónoma.

Do mesmo modo, refere-se no Anexo B que «*A plataforma de software deverá também possibilitar a integração de radares com analítica de vídeo para interior com distâncias de raio máximas de 9 metros bem como outros dispositivos ONVIF*». Ora, também neste ponto o pedido de parecer é omissivo quanto a esta funcionalidade.

¹ A título de exemplo, na alínea q) do “Desempenho de vídeo”, que integra a secção “Caraterísticas técnicas dos equipamentos”, é referido que «a Câmara possibilitará o transporte de vídeo e áudio sobre: HTTP (Unicast); HTTPS (Unicast); RTP (Unicast e Multicast); RTP over RTSP (Unicast); RTP over RTSP over HTTP (Unicast); RTP over RTSP over HTTPS (Unicast)». Tratam-se de diferentes protocolos de comunicação, que oferecem diferentes níveis de segurança da informação e que, da forma como estão elencados, não permitem aferir sobre a segurança do sistema



Especial destaque merece a referência à utilização de IA e *soft recognition*, sem que seja explicitado em que termos, sobre que pressupostos e sob que critérios estas tecnologias vão ser utilizadas. Tal omissão impede qualquer tipo de avaliação do respeito pelos limites e condições relativos à tutela da privacidade – nos termos definidos nos n.ºs 6 e 7 do artigo 7.º da Lei n.º 1/2005 –, como também impede uma ponderação, por parte do órgão com competência autorizativa, da adequação, necessidade e de respeito pela proibição do excesso quanto à utilização deste sistema de videovigilância com estes atributos.

Em rigor, a identificação de padrões como os descritos na Fundamentação (e transcritos supra, em 2.1.) implica uma análise de vídeo com confrontação com algoritmos de deteção. A funcionalidade de “procura avançada”, por exemplo, parece indiciar que o vídeo captado (e armazenado) pode ser sujeito a um varrimento para identificação de padrões, sendo certo que nada impede que a tecnologia que permite a deteção de uma determinada cor de roupa seja configurada para deteção de uma determinada cor de pele ou outra característica potencialmente discriminatória.

Ora, na Fundamentação não são descritos os algoritmos envolvidos na comparação e deteção de padrões, não é especificado quem é responsável pela definição desses padrões e também não são especificados os critérios envolvidos nesses padrões (*v.g.*, que padrões visuais o sistema usa para diferenciar um homem de uma mulher; quais são as taxas de tolerância configuradas para falsos positivos/negativos).

Acresce que a exigência do sistema apresentar ao operador «*sequências programadas de eventos em vídeo de acordo com a prioridade e de acordo com os tipos de regras violadas*» (cf. Anexo B da Fundamentação) não é suficientemente clara. Na verdade, não se entende se as “regras violadas” se referem a configurações de deteção vídeo (*v.g.*, deteção de entrada em zona) ou se correspondem a verdadeiras identificações de contraordenações, detetadas pelo sistema de análise vídeo.

Insiste-se que a falta de transparência do processo de análise da informação não só não permite, *ex ante*, compreender as consequências da sua utilização e portanto o real alcance e impacto da utilização deste sistema de videovigilância, como não permite garantir satisfatoriamente, nos termos impostos na lei, o direito de informação aos titulares dos dados.

Como se referiu supra, em 2.1., para além de não se encontrar, na Fundamentação apresentada, argumentos especificamente pensados para a utilização desta tecnologia para a finalidade de proteção de pessoas e bens e de controlo de tráfego, não estão fixadas, nem se declara que serão fixadas, as situações que justificarão a sua utilização, tão-pouco os pressupostos e critérios que estarão na base da inserção de características físicas ou outras informações relativas às pessoas, e que tipo de critérios poderão estar na base da análise inteligente da informação e da criação de perfis.

Considerando que há um conjunto de dados pessoais que estão sujeitos a um regime especialmente reforçado de proteção – os previstos no n.º 1 do artigo 6º da Lei n.º 59/2019, de 8 de agosto – e que o n.º 2 do mesmo artigo proíbe a criação de perfis que conduzam à discriminação de pessoas singulares com base nesses dados², a CNPD entende que a utilização deste tipo de tecnologia tem de ser, no mínimo, precedida de um conjunto de regras precisas para os utilizadores da mesma, de modo a limitar o risco de discriminação e de violação do artigo 6.º da referida lei.

Acrescente-se que não se percebe em que consistem os *metadados* que são enviados das câmaras, nem que tipo de pesquisas é possível efetuar sobre essa informação.

Entrando agora numa análise centrada nas características técnicas do sistema, cumpre destacar o seguinte:

- a. No que diz respeito à salvaguarda da privacidade e intimidade da vida privada, apesar de se referir, no Anexo B da Fundamentação, a aplicação de «*máscaras de privacidade*» e de nas imagens reproduzidas no Anexo A haver edifícios sinalizados com zonas negras, não há informação suficiente no pedido que permita à CNPD – e ao órgão com competência autorizativa – avaliar do respeito pelos limites previstos nos n.ºs 6 e 7 do artigo 7.º da Lei n.º 1/2005.

E quanto à captação de som, estranhamente não se encontra qualquer justificação na Fundamentação. Tendo em conta a proibição contida nos n.ºs 6 e 7 do artigo 7.º da Lei n.º 1/2005, não está demonstrada a adequação e a necessidade deste tratamento, não estão descritos os critérios a que tal

² E, no âmbito do tratamento realizado com a finalidade de gestão de tráfego, os dados pessoais previstos no n.º 1 do artigo 9.º do RGPD e os limites impostos pelo n.º 2 e 4 do artigo 22.º do mesmo diploma.

captação obedecerá, nem, a concluir-se pela sua adequação e necessidade, são indicadas quaisquer medidas mitigadoras da afetação da privacidade daí decorrente.

Nessa medida, a CNPD só pode concluir que esta funcionalidade viola o disposto nos referidos preceitos legais.

Por outro lado, refere-se ainda que as câmaras deverão estar equipadas com conexões de saída de áudio, para altifalante externo, não se encontrando na Fundamentação qualquer razão para tal exigência, nem, mais uma vez, critérios que delimitem as situações da sua utilização.

- b. Na secção “Descrição do sistema a implementar” constante do Anexo B da Fundamentação, é referida a necessidade do sistema dispor de *«alta escalabilidade e conectividade, permitindo o crescimento do sistema e sua integração com outros sistemas eletrónicos de segurança patrimonial»*. Atendendo a que não são descritas quaisquer interconexões para o tratamento de dados em apreço, não se entende quais sejam os possíveis “sistemas eletrónicos de segurança patrimonial” com os quais se põe a possibilidade de integrar.

É, pois, imprescindível que se especifiquem as eventuais interconexões de dados que o responsável pelo tratamento pretende implementar, para que a CNPD emita a competente pronúncia.

- c. No Anexo B é exigido que o sistema possua *«dupla autenticação sendo uma delas por "QR Code"»*. A este propósito, destaca-se que não é clara a aplicação que se pretende dar ao *QR Code* neste contexto, desde logo se se gera um *QR Code* único para cada autenticação, à semelhança do que algumas aplicações fazem para validar acessos.

Nessa medida, não é possível avaliar se este mecanismo confere maior ou menor segurança enquanto não for melhor concretizado.

- d. Também é exigido que o sistema tenha *«password de exportação»*.

Se a segurança do mecanismo de exportação assentar exclusivamente sobre uma palavra-passe, tal medida, por si só, não é suficiente para garantir a



confidencialidade do sistema. É ainda imprescindível que sejam fixados, em termos adequados, perfis de acesso a esta funcionalidade de exportação.

- e. No Anexo B, refere-se também que a «*Utilização de tecnologias (hardware e software) no estado de arte, incluindo análise inteligente de vídeo no software sem custos na mesma plataforma sem adicionar software terceiros. A análise inteligente de vídeo deverá vir embecida diretamente nas câmaras com análise inteligente de vídeo por metadados e deverão ter no mínimo 10 regras por câmara, a ser especificado em alguns modelos abaixo. A análise inteligente de vídeo nas câmaras deverá ser por padrões e não por "motion" ou por "advanced motion"*».

Ora, considerando que o sistema assenta numa arquitetura centralizada, não se alcança a razão por que se impõe que sejam as próprias câmaras a ter embecidas tecnologias, designadamente de análise inteligente de vídeo. Com efeito, a maior vantagem de usar este tipo de arquiteturas é tirar partido da configuração e controlo a nível central, assegurando a homogeneidade e controlo de configurações e acessos.

- f. Ainda quanto às especificações das câmaras de vídeo, refere-se a exigência de serem equipadas com cartões de memória SD (Secure Digital) para registarem vídeo «*no seu interior*». Apesar de esta exigência não estar fundamentada, admite-se que se pretenda garantir um fluxo de dados constante em caso de pontual perda de conexão com o servidor.

Contudo, considerando o risco de acesso indevido às imagens guardadas nos cartões SD, deve ser ponderada e fundamentada a instalação de sistemas de armazenamento local.

- g. Também no Anexo B da Fundamentação refere-se como característica do sistema «*Ter a possibilidade de integrar o controlo acessos do mesmo fabricante no futuro e através do mesmo fazer pesquisas de analíticas avançadas como pesquisa por aparências (face, corpo) no sistema de videovigilância*».

Fica por explicar de que forma o controlo de acessos – um conceito tradicionalmente associado ao controlo de acesso físico a infraestruturas – pode ser integrado com pesquisas avançadas num sistema de videovigilância.

Ainda sobre o controlo de acessos, mas agora relacionado com a segurança do servidor, é referido que «*a plataforma deverá ter dupla autenticação para a visualização do vídeo gravado*». Para garantia da confidencialidade dos dados do sistema, o mecanismo de dupla autenticação deve estender-se a todos os tipos de acessos, quer sejam os feitos para acesso às imagens gravadas, imagens em tempo real ou alteração de configurações

- h. Quanto aos mecanismos de auditoria do sistema, apenas é feita referência a *logs* de acesso.

Ora, os n.ºs 3 e 4 do artigo 4.º da Portaria n.º 372/2012, exige *logs* que registem toda a atividade dos utilizadores, bem como a alteração de configurações do sistema (*v.g.*, alteração da área de máscaras de visualização). Esta exigência está reforçada no artigo 27.º da Lei n.º 59/2019, de 8 de agosto, que impõe os registos cronológicos das operações enunciadas nas alíneas *a)* a *g)* do n.º 1 do mesmo artigo, bem como a sua fundamentação.

- i. Importa ainda referir que os «Requisitos mínimos dos computadores» exigidos para o Centro de Controlo de Portimão e para o Centro de Visionamento Principal são os mesmos. Todavia, na medida em que o primeiro só pode proceder à visualização de imagens (nos termos declarados na Fundamentação), os computadores destinados a esse local não devem dispor de *hardware* de «Leitor/Gravador DVD» e portas USB que constam nas especificações. A existirem, estas interfaces devem estar inibidas.

2.3. Outros aspetos do funcionamento do sistema

Assinala-se ainda que, no Anexo B, se exige que o sistema permita «*pôr qualquer câmara em "stand by" com as devidas credenciais do responsável de tratamento dos dados (Encarregado de Proteção dos Dados)*».

Sublinha-se que um tal requisito está em manifesta contradição com o regime de proteção de dados pessoais e com as funções de Encarregado de Proteção dos Dados (cf. o artigo 35.º da Lei n.º 59/2019, de 8 de agosto, artigo 39.º do RGPD, e artigo 11.º da Lei n.º 58/2019, de 8 de agosto). Se, por um lado, não cabe a este efetuar alterações às condições do tratamento, por outro, é ilícito que este opere «com as devidas credenciais do responsável de tratamento dos dados».

Importa ainda atentar num outro aspeto. Na Fundamentação, a propósito dos «mecanismos tendentes a assegurar o correto uso dos dados registados», esclarece-se que no Centro de Controlo de Portimão, instalado na Esquadra de Portimão, o controlo de acessos aos ecrãs de monitorização será garantido por um «*elemento policial que se encontra em permanência naquele ponto de passagem*». Também quanto ao Centro de Visionamento Principal, sito no comando Distrital de Faro, é referido que o acesso é restrito aos operadores de comunicações. Em qualquer dos casos, não são explicitadas medidas aptas a garantir o controlo de acessos.

Deste modo, recomenda-se a adoção de um mecanismo de controlo que permita auditar os acessos às instalações.

2.4. Os direitos de informação, de acesso e de eliminação dos dados

Em relação aos direitos dos titulares dos dados, chama-se a atenção para o facto de eles estarem hoje definidos na Lei n.º 59/2019, de 8 de agosto, que aprova as regras relativas ao tratamento de dados pessoais para efeitos de prevenção, deteção, investigação ou repressão de infrações penais ou de execução de sanções penais, transpondo a Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016. Tem-se aqui especificamente em vista o direito de informação dos titulares dos dados, mais densificado no artigo 14.º da Lei n.º 59/2019, de 8 de agosto.

Assinala-se como positivo o facto de, neste novo projeto agora apreciado, além de se declarar que os modelos de aviso e simbologia a utilizar respeitam o estatuído na Portaria n.º 373/2012, de 16 de novembro, se acrescenta que será publicada informação sobre a instalação do sistema de videovigilância em meios digitais de divulgação de informação da PSP (cf. Anexo E da Fundamentação).

Todavia, considerando as tecnologias IA e *soft recognition* que se pretende associar na análise da informação que o sistema recolhe, é evidente que o direito de informação tem se ser muito mais densificado, pelo menos, quando em causa esteja a prossecução da gestão do tráfego e prevenção e repressão de infrações estradais que não constituam crime – porque o direito de informação segue, aqui, as regras do artigo 14.º do RGPD.

No que respeita aos direitos de acesso e eliminação dos dados, declara-se, no Anexo C da Fundamentação, que serão garantidos em conformidade com o disposto no n.º 1 do artigo 10.º da Lei n.º 1/2015.

III. CONCLUSÃO

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

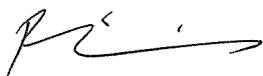
1. Entende ser imprescindível o cumprimento do dever, previsto no artigo 29.º da Lei n.º 59/2019, de 8 de agosto, bem como no n.º 1 e na alínea *c*) do n.º 3 do artigo 35.º do RGPD, de realizar uma prévia avaliação de impacto do tratamento de dados pessoais sobre os direitos, liberdades e garantias das pessoas, no âmbito do presente procedimento autorizativo, em especial quanto à utilização de tecnologias de Inteligência Artificial e *soft recognition*;
2. No âmbito e na sequência da referida avaliação de impacto, considera especialmente pertinente:
 - i. A ponderação dos diferentes direitos e interesses em tensão, não apenas quanto ao sistema de videovigilância com a abrangência declarada, mas também quanto ao nível de intrusão na privacidade e liberdade dos cidadãos, bem como no direito à não discriminação, decorrente da utilização de tecnologias de Inteligência Artificial e *soft recognition*, em função de cada uma das finalidades visadas – a saber, a proteção de pessoas e bens e a prevenção e repressão de infrações estradais e controlo de tráfego rodoviário;

- ii. A compreensão de que o cumprimento do regime jurídico de proteção de dados e da vida privada se atinge pela forma como os tratamentos de dados são concebidos e implementados e não pela utilização de um tipo específico de tecnologia;
 - iii. A definição prévia de um conjunto de regras vinculativas para a utilização destas tecnologias, de modo a limitar o risco de discriminação e de violação do artigo 6.º da Lei n.º 59/2019, de 8 de agosto;
 - iv. A apresentação de fundamentação e de elementos que permitam compreender o real alcance e impacto do emprego daquelas tecnologias de análise da informação no contexto deste sistema de videovigilância, sob pena de não ser possível o juízo de proporcionalidade por parte do órgão com competência autorizativa, nem o juízo da CNPD a emitir quanto aos limites definidos nos n.ºs 6 e 7 do artigo 7.º da Lei n.º 1/2005;
3. No âmbito e na sequência da avaliação de impacto, recomenda que se atenda às observações contidas nos pontos 2.2 a 2.4.

Nestes termos, atendendo especialmente que a utilização de um sistema de videovigilância com as características já destacadas representa um elevado risco para a privacidade dos cidadãos, não só pela quantidade e pelo tipo de informação que é possível recolher a partir das imagens captadas e gravadas, mas também pela opacidade de que se reveste o processo de definição de padrões de análise e a sua deteção, a CNPD emite parecer negativo quanto ao pedido de autorização de instalação de um sistema de videovigilância na cidade de Portimão.

Sublinha-se ainda a necessidade de nova consulta da CNPD, quanto aos aspetos omissos no pedido agora apresentado, e sobre os quais, nos termos do n.º 2 do artigo 3.º da Lei n.º 1/2005, é obrigatória a sua pronúncia.

Lisboa, 27 de dezembro de 2019



Filipa Calvão (Presidente, que relatou)