

## PARECER/2020/145

### I. PEDIDO

Em 22 de setembro de 2020, por despacho do Secretário de Estado Adjunto e da Administração Interna, foi solicitado parecer à Comissão Nacional de Proteção de Dados (CNPD) sobre o pedido de autorização de instalação de um sistema de videovigilância na cidade de Lisboa, submetido pela Polícia de Segurança Pública (PSP).

A CNPD aprecia o pedido 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".

Considerando que o processamento de dados produzidos por este sistema pode resultar em elevado risco para os direitos e liberdades das pessoa e porque o mesmo implica um controlo sistemático em larga escala, foi efetuada a avaliação de impacto sobre proteção de dados (AIPD) para o tratamento de dados em questão, remetida à CNPD junto com o pedido de autorização e respetivos anexos, em conformidade com o estatuído no artigo 29.º da 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.

É com base nas informações constantes dessa AIPD, bem como da Fundamentação que acompanha o pedido, que a CNPD emite o presente parecer.

### 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 Lisboa para a finalidade de proteção de pessoas e bens e prevenção de crimes**

Pretende-se a instalação de 216 câmaras de videovigilância, divididas em 16 zonas do concelho de Lisboa. Declara-se que o sistema apenas procederá à gravação de imagens, sublinhando-se que não será utilizada a capacidade de gravação de som.

### **2.1. O impacto sobre a privacidade dentro dos edifícios habitacionais**

Ainda que não caiba, 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 Lisboa implica um tratamento de dados pessoais que, pelo seu âmbito e extensão, é suscetível de afetar significativamente a vida privada das pessoas que circulem ou se encontrem naquela cidade. Importa, por isso, determo-nos neste ponto.

No Anexo A da Fundamentação descrevem-se as áreas da cidade de Lisboa objeto de vigilância e apresenta-se a captura da área de visualização de cada câmara. Nessas imagens, são apresentadas áreas delimitadas com elipses azuis que parecem corresponder a zonas com janelas ou entradas de edifícios e que, presume-se, pois não é referido, são as zonas de bloqueio digital de gravação. Com efeito, declara-se no Anexo B, relativo às características técnicas gerais dos equipamentos de videovigilância, que «o *software* dessas mesmas câmaras possibilitará a colocação ilimitada de máscaras 3D individualmente configuráveis para ocultar as áreas definidas das imagens», e que as máscaras serão dinamicamente ajustadas para se manterem mesmo durante a aplicação da operação de *zoom*. Sendo aplicadas antes do fluxo de vídeo, vão surgir também nos ficheiros gravados.

Também no Anexo B, são identificados três tipos distintos de câmaras, a saber: câmara 4K fixa (8MP), câmara 6K fixa (24MP) e câmara PTZ FULL HD (2MP).

Ainda que, a partir da documentação apresentada, não seja possível identificar os tipos de câmaras – de entre os três elencados (com diferentes capacidades) – que serão instalados em cada local, e portanto seja difícil avaliar o real impacto sobre a privacidade, a aplicação de máscaras atenua o impacto sobre a privacidade no acesso e dentro dos edifícios, desde que o sistema não permita a sua desativação, edição ou eliminação pelos utilizadores do sistema.

Ainda quanto ao impacto na privacidade, considerando a afirmação de que *não será utilizada a capacidade de gravação de som*, importa garantir que o sistema não permita a utilização dessa capacidade.

## 2.2. Das características técnicas do sistema

Considerando agora as características técnicas do sistema de videovigilância, importa verificar se estão cumpridos os diferentes requisitos legais e regulamentares aplicáveis. Recorda-se que tais requisitos reportam-se à segurança da recolha, transmissão e conservação das imagens, de modo a garantir a confidencialidade, a autenticidade e integridade das imagens gravadas, bem como a auditabilidade 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 equipamentos. 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.

Entrando agora numa análise centrada nas características técnicas do sistema, cumpre destacar os seguintes aspetos do tratamento de dados pessoais.

- a. De acordo com o declarado no Anexo B da Fundamentação, relativo às características técnicas do equipamento, o sistema permite «desabilitar *zoom*» por determinados utilizadores, ou níveis de utilizadores.

Recomenda-se que se assegure o específico registo (*log*) da ativação do *zoom*, para que se possa auditar a utilização desta funcionalidade e a sua necessidade.

- b. No 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. 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.

Atendendo a que a conservação das imagens nos cartões SD locais potencia o risco de acesso indevido, recomenda-se que o responsável pelo tratamento garanta que a informação guardada no cartão SD se restringe aos últimos segundos de captação de vídeo, de forma a minorar o risco em caso de acesso indevido ou furto da câmara.

- e. Nem na Fundamentação, nem na AIPD há referência à existência de um servidor ou *storage* que permita efetuar o *backup* quer das gravações, quer dos *logs* de sistema e registos de acesso, para tornar possível a recuperação desses dados em caso de falha do servidor principal.

Recomenda-se a implementação de um mecanismo de redundância que possa garantir a continuidade da gravação e do funcionamento do sistema em qualquer situação imprevista.

- f. Embora na AIPD se refira que haverá «controlo dos suportes de dados», não é esclarecido se esse controlo será feito também à entrada da sala onde se encontra o servidor principal e ecrãs de monitorização, não permitindo que os operadores e outras pessoas que aí acedam levem consigo suportes externos, ou se existem mecanismos que garantam que os postos de monitorização são utilizados exclusivamente para o visionamento de imagens.

Deste modo, recomenda-se que as máquinas tenham salvaguardas para prevenir a cópia de imagens e armazenamento em suportes externos, de modo a respeitar-se o disposto no artigo 9.º da Lei n.º 1/2005.

### 2.3. Os direitos de informação, de acesso e de eliminação dos dados

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; quanto ao direito de informação, declara-se cumprir o estatuído na Portaria n.º 373/2012, de 16 de novembro.

Chama-se, contudo, a atenção para o facto de os direitos dos titulares dos dados 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, do que aquilo que o artigo 4.º da Lei n.º 1/2005 previa.

Enquanto o legislador nacional não procede à atualização dos regimes especiais, de modo a garantir a sua conformidade com o disposto na Diretiva (UE) 2016/680, que a Lei n.º 59/2019, de 8 de agosto, transpõe, este artigo 4.º da Lei n.º 1/2005 tem de ser interpretado e aplicado de forma a respeitar as exigências do novo regime de proteção de dados pessoais.

Não é por isso suficiente a declaração de que os modelos de aviso e simbologia a utilizar respeitam o estatuído na Portaria n.º 373/2012, de 16 de novembro, devendo ainda garantir-se o direito de informação previsto no artigo 14.º da Lei n.º 59/2019, através da disponibilização de outra informação sobre a instalação do sistema de videovigilância em meios digitais de divulgação de informação da PSP, em especial, tendo em conta que se pretende associar as tecnologias de analítica de vídeo na análise da informação que o sistema recolhe.

## 2.4. Outros aspetos do tratamento de dados pessoais decorrente da utilização do sistema

### *2.4.1. O responsável pelo tratamento e o encarregado de proteção de dados*

Ao longo do pedido (da Fundamentação que o acompanha) há várias referências à intervenção do encarregado de proteção de dados no tratamento de dados pessoais decorrente da utilização do sistema de videovigilância, em termos que suscitam as maiores reservas quanto ao respeito pelos artigos 34.º, n.º 1, e 35.º da Lei n.º 59/2019, de 8 de agosto.

Na verdade, não apenas se indica no texto do pedido de autorização que «*Todas as operações de programação e alteração de operação serão realizadas pelo encarregado de proteção de dados*» (cf. alínea *g*) do referido pedido), como no Anexo B da Fundamentação 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)*». Na AIPD refere-se ainda que «*a extração de gravações das imagens vídeo dependerá de despacho prévio de autorização pelo encarregado da proteção de dados*». Finalmente, e mais estranho ainda, no Anexo C, o encarregado de proteção de dados da PSP é também indicado como responsável pelo tratamento dos dados.

Importa ter presente que às funções do Encarregado de Proteção de Dados, que se encontram exemplificadas no artigo 35.º da Lei n.º 59/2019, de 8 de agosto, não é impossível acrescerem outras funções, mas estas não podem adulterar a sua missão de *«assistir [o responsável pelo tratamento] no controlo do cumprimento das obrigações»*, nos termos do n.º 1 do artigo 34.º da mesma lei, pelo que em caso algum podem implicar uma partilha de responsabilidade pelo tratamento de dados e nem uma transferência ou partilha da responsabilidade pelo cumprimento das diferentes obrigações legais que recaem sobre o responsável pelo tratamento. O encarregado de proteção de dados desempenha uma função essencialmente consultiva e de auditoria, não podendo por isso tomar as decisões sobre o tratamento, pois desse modo estaria a recair sobre ele a responsabilidade por tais decisões – em clara contradição com o estatuído nos artigos 20.º e seguintes da Lei n.º 59/2019, de 8 de agosto.

Assim, não se afastando a solução de, quanto a uma série de operações concretas de tratamento de dados no âmbito do presente sistema de videovigilância, se prever a intervenção do encarregado de proteção de dados, entende a CNPD ser imprescindível que a mesma não assuma carácter decisório ou autorizativo, mas antes cariz consultivo (portanto, prevendo-se a necessidade de parecer do encarregado, em vez de lhe atribuir o poder de autorização dessas operações).

#### *2.4.2. Relação de subcontratação*

Quanto à relação de subcontratação, na documentação disponibilizada apenas se esclarece que a Câmara Municipal de Lisboa (CML) *«é a responsável pela manutenção do sistema, a qual deverá assegurar todos os custos de manutenção, reparação e conservação dos equipamentos»* – cf. anexo I da Fundamentação.

Importa, a este propósito, sublinhar que a relação de subcontratação, no que ao tratamento de dados pessoais diz respeito, se estabelece entre a PSP (responsável pelo tratamento) e a entidade terceira que venha a ser subcontratada, independentemente da entidade pública que financia a aquisição do equipamento. Assim, cabe à PSP determinar, não apenas quais as características dos equipamentos que compõem o sistema de videovigilância a adquirir, como também as garantias suficientes de execução de medidas técnicas e organizativas adequadas a prosseguir a finalidade do tratamento que devem ser apresentadas por um subcontratante na gestão da



manutenção, reparação e conservação dos meios através dos quais o tratamento é realizado. É o que resulta do n.º 1 do artigo 23.º da Lei n.º 59/2019, de 8 de agosto.

Ainda que o procedimento para a adjudicação do contrato de subcontratação, bem como os custos com a execução do contrato de subcontratação, sejam assumidos pela CML, importa garantir que no contrato de subcontratação também a PSP surja como parte e que, nos termos do respetivo clausulado, seja garantido que a PSP controle com autonomia o sistema, por ser por ele responsável nos termos da lei, ficando o subcontratante vinculado à PSP.

Se os serviços de manutenção, atualização, reparação e conservação dos meios, através dos quais o tratamento é realizado, for objeto do contrato de aquisição do equipamento, é imprescindível que o caderno de encargos e, consequentemente, o contrato prevejam o papel da PSP como responsável pelo tratamento e, nessa medida, o dever de prestação de serviço e de reporte do adjudicatário, enquanto subcontratante, direta e exclusivamente à PSP.

## 2.5. O recurso a tecnologia de analítica de vídeo

Embora nada seja referido na AIPD quanto ao recurso a tecnologia de Inteligência Artificial ou *video analytics*, a verdade é que no Anexo B da Fundamentação há referência explícita, nos três tipos de câmaras, à exigência de «*capacidade de medir quantos pixéis estão numa determinada cena para melhor qualificar a analítica de vídeo do espaço ou área; [d]isponibilizar na matriz de vídeo do operador as sequências programadas de eventos em vídeo de acordo com a prioridade e de acordo com os tipos de regras violadas*».

Ora, estas características dos equipamentos revelam que o sistema de videovigilância implica a utilização de tecnologia avançada de analítica de imagens, sem que se perceba quais sejam os critérios de prioridade ou os tipos de regras violadas.

Em rigor, as características acima descritas indiciam a identificação de padrões e uma análise de vídeo com confrontação com algoritmos de deteção. Ora, na Fundamentação não são descritos os algoritmos envolvidos na comparação, nem são especificados os critérios, tão-pouco quem é responsável pela definição desses critérios.

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 6.º 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 dados, a CNPD entende que, nos termos em que vem instruído o procedimento, não é possível avaliar e concluir sobre a adequação, necessidade e de respeito pela proibição do excesso quanto à utilização do sistema de videovigilância com estes atributos.

Sublinha-se, por isso, a imprescindibilidade de a utilização deste tipo de tecnologia 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, as quais, na falta de diploma normativo, têm de constar do ato administrativo autorizativo.

### III. CONCLUSÃO

1. 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 Lisboa, a CNPD, com os argumentos acima expostos, recomenda o seguinte:

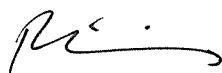
- a. Para que se possa considerar suficientemente mitigado o impacto sobre a privacidade no acesso e dentro dos edifícios, nos termos exigidos pelo artigo 7.º da Lei n.º 1/2005, o sistema tem de garantir que não é possível a desativação, edição ou eliminação das máscaras pelos utilizadores do sistema, nem a utilização da capacidade de gravação de som;
- b. Que sejam seguidas as observações estabelecidas supra, no ponto 2.2.;
- c. Em cumprimento do disposto no artigo 14.º da Lei n.º 59/2019, de 8 de agosto, que a informação prevista na Portaria n.º 373/2012, de 16 de novembro, seja complementada com outra informação sobre a instalação do sistema de videovigilância em meios digitais de divulgação de informação da PSP;
- d. Sob pena de se violar o disposto no n.º 1 do artigo 34.º da Lei n.º 59/2019, de 8 de agosto, bem como as normas nela previstas relativas a obrigações específicas do responsável pelo tratamento de dados pessoais, a intervenção do

encarregado de proteção de dados em determinadas operações de tratamento de dados não pode assumir caráter decisório ou autorizativo, mas antes cariz consultivo;

- e. Como a contratação de serviços de manutenção, atualização, reparação e conservação dos meios através dos quais o tratamento é realizado corresponde a uma subcontratação regulada no artigo 23.º da Lei n.º 59/2019, de 8 de agosto, é à PSP, enquanto responsável pelo tratamento, que a empresa contratada está vinculada e a quem presta o serviço, pelo que, quer tais serviços constem do contrato de aquisição do equipamento, quer constem de contrato autónomo, é imprescindível que o caderno de encargos e, consequentemente, o contrato prevejam o papel da PSP como responsável pelo tratamento e, nessa medida, o dever de prestação de serviço e de reporte do adjudicatário, enquanto subcontratante, direta e exclusivamente à PSP.

2. A referência à utilização de tecnologia de analítica de vídeo, tal como descrita no Anexo B da Fundamentação, não vem acompanhada da definição dos critérios ou padrões de análise, nem de limites à sua definição, tão-pouco da identificação de quem os vai definir, pelo que tendo em conta o impacto na privacidade e o risco de discriminação decorrentes da sua utilização, a CNPD entende que não é possível avaliar e garantir a proporcionalidade do tratamento de dados pessoais decorrente da utilização deste sistema de videovigilância com estes atributos; chama por isso a atenção para a necessidade de a utilização deste tipo de tecnologia 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, as quais, na falta de diploma normativo, têm de constar do ato administrativo autorizativo.

Aprovado na reunião de 16 de dezembro de 2020



Filipa Calvão (Presidente)