

PARECER/2019/93

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 para alargamento do sistema de videovigilância no Município de Leiria, 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 no Município de Leiria 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, o alargamento do sistema de videovigilância no Município de Leiria 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 no concelho de Leiria. 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 a aumentar o número de câmaras em relação ao atual sistema de videovigilância, mais do que triplicando o número atual de câmaras – às atuais dezanove câmaras pretende-se somar quarenta e duas câmaras (cf. pág. 2 e Anexo A, pág. 7, da Fundamentação) –, num total de sessenta e uma câmaras de videovigilância. Para além da extensão do tratamento de dados pessoais, deve aqui considerar-se ainda 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, a que acresce a possibilidade de captação de som.

Mas sobretudo, destaca-se a circunstância de as câmaras disporem de «*tecnologia de deteção avançada de padrão de vídeo e leitura de matrículas*» e de o sistema estar dotado da funcionalidade de «*analítica de vídeo e reconhecimento de matrículas*», «*deteção de movimento e filtro de pesquisa por movimento ou padrão, com acionamento de alarmes e marcadores*» e «*analítica de vídeo com auto-aprendizagem*» (cf. Anexo B, ponto 1, da Fundamentação). Ora, a utilização de tecnologia de *soft recognition*, e até de *machine learning*, pode afigurar-se útil em determinadas circunstâncias, para a prevenção e repressão criminal e, portanto, poder ser eventualmente tida como adequada para a finalidade de proteção de pessoas e bens. O que não se afigura adequada ou, pelo menos, necessária é a sua utilização para a gestão de tráfego rodoviário, finalidade que é também visada neste tratamento de dados conforme o declarado na fundamentação (cf. pág. 2 da Fundamentação).

Na verdade, e começando pela tecnologia de *soft recognition*, não se alcança como se pode, por via da inserção no sistema de videovigilância 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. Em especial, quando se considera que, em relação a várias câmaras, só se apresentam argumentos para a sua instalação relativos a «controlo de tráfego», declarando-se também, mas apenas secundariamente, a proteção de pessoas e bens como finalidade a prosseguir, parece difícil concluir pela adequação e necessidade daquela tecnologia neste sistema de videovigilância (cf., por exemplo, Anexo A, págs. 36 a 44, e 70 da Fundamentação).



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 específica tecnologia e funcionalidade, invocando-se genericamente (para todo o sistema) a necessidade de repressão e também de prevenção de crimes, por força do «efeito dissuasor na prática de determinados ilícitos criminais e condutas anti-sociais» (pág. 4), a que se junta sinistralidade rodoviária e «a constante ameaça terrorista internacional sobre os países ocidentais» (cf. pág. 30). Portanto, um conjunto finalidades bem distintas, que não justificam evidentemente medidas restritivas da privacidade de igual intensidade – havendo mesmo pontos na Fundamentação em que se invoca o combate a meras «incivildades» (págs. 2 e 22).

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 referência à utilização de *analítica de vídeo com auto aprendizagem* 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 inteligência artificial (IA) e visão computacional. Tal realidade pode, *prima facie*, parecer não ser muito diferente dos métodos tradicionais de análise de informação, mas a IA com autoaprendizagem não a analisa do modo como foi inicialmente programada; ao contrário, a sua novidade traduz-se na capacidade de as máquinas “aprenderem” com a informação que vão tratando, de forma a responderem autonomamente (de modo “inteligente”), gerando informação nova. 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 na vertente de *machine learning*, 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 no concelho de Leiria, mas também especificamente quanto às tecnologias de *soft recognition* e de *machine learning*, 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*, de IA e de *machine learning*, 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 no concelho de Leiria, 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 grande parte das câmaras visa a título principal a gestão do tráfego (e apenas secundária e residualmente se invoca a proteção de pessoas e bens), 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 alargamento do sistema de videovigilância não vem suficientemente instruído, não permitindo por isso à CNPD avaliar do respeito pelos diferentes aspetos de regime indicados 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.

Esta omissão da descrição de importantes características do sistema não pode ser colmatada, porventura, por via de remissão para os elementos que instruíram o

procedimento autorizativo anterior e que originou o despacho n.º 7531/2015, da Secretária de Estado Adjunta e da Administração, que autorizou a instalação de 19 câmaras, uma vez que os elementos apresentados à CNPD para emissão do respetivo parecer já então eram insuficientes, como se assinalou no Parecer n.º 34/2014, de 6 de maio¹.

Em especial, a referência à utilização de IA, *machine learning* e *soft recognition*, sem explicitar em que termos, sobre que pressupostos e sob que critérios estas tecnologias vão ser utilizadas, 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.

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

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 ser evidente a sua não adequação e a sua desnecessidade para a gestão de tráfego rodoviário, 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 da informação em autoaprendizagem 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 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

¹ Disponível em https://www.cnpd.pt/bin/decisooes/Par/40_34_2014.pdf

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.

- b. A Fundamentação agora apresentada é omissa quanto a medidas de segurança aplicadas à informação transmitida entre as câmaras de vídeo e o servidor central. A CNPD recomenda, por isso, que, na sequência da avaliação de impacto sobre a proteção dos dados, se definam as medidas de segurança adequadas à transmissão da informação.
- c. No que diz respeito à salvaguarda da privacidade e intimidade da vida privada, indica-se, no Anexo B da Fundamentação, como requisitos mínimos das câmaras de videovigilância que as mesmas têm *«capacidade de programação de filtros na captação de imagem e som (para evitar captação de imagem e som em circunstâncias não admissíveis, em respeito pelo direito à privacidade)»* (cf. ponto 1) e, quanto ao *software* de instalação, a aptidão para *«criar/editar/eliminar filtros de imagem/som, nomeadamente a colocação de máscaras para evitar a captação e gravação de imagens nas zonas em que se verifique que o alcance do zoom do sistema possa colidir com o direito à privacidade das pessoas»* (cf. ponto 4).

Mais se declara, no Anexo F, que o *«equipamento e software utilizados garantirão a utilização de máscaras/filtros para não captar e gravar imagens de locais privados, impedindo a visualização de, designadamente, portas, janelas e varandas, garantindo o direito à privacidade das pessoas; e o barramento de som, só desbloqueado em circunstâncias em que se verifique uma situação de perigo concreto para a segurança das pessoas e bens»*.

Ora, em face do declarado, não pode afirmar-se que a privacidade e os demais direitos fundamentais das pessoas eventualmente abrangidas pelo raio de captação das câmaras ficam salvaguardados.

Por um lado, não se explicitam se as máscaras a aplicar são físicas ou lógicas, sublinhando-se aqui que, por se tratarem de câmaras PTZ, com capacidade para

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.

ampliação de imagem e rotação, as máscaras mais adequadas se afiguram ser lógicas. De resto, apenas quanto a algumas câmaras se exemplifica onde serão colocadas máscaras (*v.g.*, pág. 70 da Fundamentação), pelo que não é possível, pela análise da Fundamentação apresentada, determinar se serão colocadas em todos os locais onde as mesmas são necessárias, nem se serão eficazes. Nessa medida, fica prejudicada a avaliação da CNPD relativamente ao respeito pelos limites definidos no n.º 6 do artigo 7.º da Lei n.º 1/2005.

Por outro lado, a previsão da funcionalidade de editar e eliminar os filtros de imagem/som, aparentemente por qualquer utilizador do sistema, sem que se definam, de antemão, as circunstâncias justificadoras de uma tal medida, não oferece garantias para a tutela dos direitos, liberdades e garantias das pessoas. E quanto à captação de som – para a qual, estranhamente, não se encontra justificação na Fundamentação –, a falta de densificação das circunstâncias em que o barramento de som pode ser desbloqueado não permite avaliar se a compressão do direito ao respeito pela vida privada é proporcionado, como impõe o n.º 7 do artigo 7.º da Lei n.º 1/2005.

- d. No Anexo B, ponto 2, indica-se como requisitos mínimos do servidor de vídeo, «*Taxa de gravação e de reprodução e transmissão ao vivo (enquanto grava em simultâneo) até 450 Mbps*».

Admitindo-se que tal signifique a possibilidade de fazer *reprodução* das imagens gravadas, sublinha-se que tal funcionalidade parece violar o disposto no n.º 1 do artigo 9.º da Lei n.º 1/2015, que impõe a codificação do registo das imagens, precisamente para impedir que os agentes autorizados a visualizar as imagens em tempo real possam aceder às imagens gravadas ou reproduzi-las. De todo o modo, sempre será imprescindível a implementação de *logs* para que seja possível auditar as intervenções nas imagens gravadas.

Por essa razão, a CNPD recomenda que se adotem medidas que garantam o respeito pelo disposto no n.º 1 do artigo 9.º da Lei n.º 1/2015.

2.3. 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, pág. 82 da Fundamentação).

Todavia, considerando as tecnologias IA, *machine learning* e *soft recognition* que se pretende associar na análise da informação que o sistema recolhe, é evidente que o direito de informação tem de ser muito mais densificado, pelo menos, quando em causa esteja a prossecução da gestão do tráfego – 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 F 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 do alargamento do sistema de videovigilância no Município de Leiria, 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, *machine learning* 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 extensão 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, *machine learning* e *soft recognition*, em função de cada uma das finalidades visadas – a saber, a proteção de pessoas e bens e o 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;

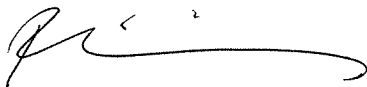
3. No âmbito e na sequência da avaliação de impacto, recomenda:
 - i. A definição e implementação de medidas de segurança adequadas à transmissão das imagens entre as câmaras e o servidor central;
 - ii. A especificação do tipo de filtros e máscaras a aplicar às imagens e som, para mitigar o impacto na privacidade, sob pena de não ser possível à CNPD, tão-pouco ao órgão com competência autorizativa, avaliar do respeito pelos limites definidos nos n.ºs 6 e 7 do artigo 7.º da Lei n.º 1/2005;

- iii. Adoção de medidas que garantam o respeito pelo disposto no n.º 1 do artigo 9.º da Lei n.º 1/2015, no que diz respeito à reprodução das imagens;
- iv. A densificação do direito de informação, também à luz do disposto no artigo 14.º do RGPD, tendo em conta a utilização de tecnologias IA, *machine learning* e *soft recognition*, em especial quanto às câmaras que visam a gestão do tráfego rodoviário.

Nestes termos, a CNPD emite parecer negativo quanto ao pedido de autorização de alargamento do sistema de videovigilância no Município de Leiria.

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)