CNPD
Comissão Nacional
de Proteção de Dados

PARECER/2024/30

I. Pedido

1. A Comissão Nacional de Proteção de Dados (CNPD) emitiu, a 26 de junho 2024, o PARECER/2024/19, na sequência do pedido apresentado, ao abrigo do disposto no n.º 3 do artigo 5º, da Lei n.º 95/2021, de 29 de dezembro, pela Secretária de Estado Adjunta e da Administração Interna relativo ao alargamento do sistema de videovigilância no Município do Porto com instalação de mais 117 câmaras.

2. A 25 de julho de 2024 foi recebido na CNPD o ofício, datado de 22 de julho de 2024, do Secretário de Estado da Administração Interna a remeter, *"[e]m resposta ao Parecer/2024/19 (…), o pedido de autorização de alargamento do sistema de videovigilância da cidade do Porto, devidamente reformulado* (…)".

3. O pedido vem acompanhado de 9 anexos:

a. Fundamentos justificativos da necessidade e conveniência da instalação do sistema de vigilância por câmaras de vídeo;
b. Identificação do local e da área abrangidos pela captação;
c. Identificação dos pontos de instalação das câmaras;
d. Descrição dos critérios utilizados no sistema de gestão analítica dos dados captados;
e. Características técnicas do equipamento utilizado;
f. Mecanismos tendentes a assegurar o correto uso dos dados registados;
g. Identificação do serviço da força de segurança responsável pela conservação e tratamento dos dados;
h. Procedimentos de informação ao público sobre a existência do sistema;
i. Avaliação de impacto sobre a proteção de dados.

4. Não constam do pedido os seguintes elementos:

a. O contrato de aquisição do sistema de videovigilância celebrado pelo Município, que inclui a manutenção do sistema, a reparação e a substituição dos equipamentos avariados;
b. O protocolo de cooperação ou documento equivalente celebrado entre a PSP e o Município do Porto onde deverão ser detalhados os termos de uso das instalações onde o sistema se encontra instalado.

5. Atendendo a que não foi remetida informação constante do acima referido contrato de aquisição do sistema de videovigilância foi feita uma consulta do Portal Base e recolhidos alguns elementos relacionados com os procedimentos de contratação do sistema em causa, a saber:

a. CPI/8/2023/DMC, publicado a 18-04-2024, com data do contrato de 29-01-2024;
b. CPI/14/2022/DMC, publicado a 24-01-2023, com data do contrato de 21-11-2022.

II. Apreciação

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

6. Nos termos do n.º 3 do artigo 5.º da Lei n.º 95/2021, de 29 de dezembro (doravante Lei n.º 95/2021), o parecer da CNPD, emitido dentro do prazo fixado no n.º 4 do mesmo artigo, em conjugação com as alíneas b) e c) do artigo 87.º do Código do Procedimento Administrativo, restringe-se à pronúncia relativa à conformidade da proposta do sistema com segurança do tratamento dos dados recolhidos e com o previsto nos nºs 4 a 6 do artigo 4.º e nos artigos 16.º, 18.º a 20.º e 22.º do mesmo diploma legal.

7. É, por isso, também objeto de parecer da CNPD, de acordo com os acima referidos preceitos legais, o respeito pela proibição de instalação e utilização de câmaras em áreas que, apesar de localizadas em locais públicos, sejam, pela sua natureza, destinadas a ser utilizadas em resguardo, e ainda a instalação e utilização de câmaras quando a captação de imagens e de sons abranja interior de casa ou edifício habitado ou sua dependência, ou de estabelecimentos hoteleiros ou similares e quando essa captação afete, e modo direto e imediato, a esfera da reserva da vida privada íntima dos cidadãos.

8. É ainda objeto de parecer da CNPD a recolha e processamento dos dados pessoais, em especial se realizado através de gestão analítica dos dados captados, por aplicação de critérios técnicos, bem como pelo respeito pelas condições e limites de conservação das gravações.

9. Deve também a CNPD verificar se estão asseguradas, a todas as pessoas que figurem em gravações obtidas pelo sistema, as condições para o exercício dos de acesso e eliminação, quando aplicáveis, e garantido o direito de informação.

CNPD
Comissão Nacional
de Proteção de Dados

ii. O atual pedido *vs* o anterior pedido

10. No seu PARECER/2024/19, de 26 de junho, a CNPD, em suma, suscitou as seguintes questões:

i. A necessidade de respeitar o n.º 4 do artigo 4.º da Lei n.º 95/2021 que proíbe "*a instalação e a utilização de câmaras (…) em áreas que, apesar de situadas em locais públicos, sejam, pela sua natureza, destinadas a ser utilizadas em resguardo*" (cf. ponto 18 do Parecer);

ii. A necessidade de ser assegurada, através da aplicação de máscaras digitais, a não captação de imagens que abranjam "*o interior de casa ou edifício habitado ou sua dependência, ou de estabelecimentos hoteleiros e similares (…)*" (cf. pontos 18 e 19 do Parecer);

iii. A impossibilidade de a CNPD se pronunciar sobre a utilização da analítica de vídeo, por desconhecer os concretos critérios para a sua utilização (cf. pontos 20 e 21 do Parecer); e

iv. A ausência de informação sobre os registos cronológicos para fins de auditoria, impossibilitando a pronúncia sobre a licitude do sistema (cf. ponto 22 do Parecer).

11. A documentação que agora acompanha o pedido enviado pretende dar resposta a algumas das observações acima indicadas, mas é sobretudo relevante ter sido remetida a Avaliação de Impacto sobre a Proteção de Dados (AIPD[1]).

iii. Do tratamento decorrente da videovigilância no Município do Porto

12. Em causa está um tratamento de dados decorrente do pedido de autorização de alargamento do sistema de videovigilância no Município do Porto que, de acordo com o declarado, pretende aditar 117 novas câmaras às 79 já existentes. Deste modo, o sistema comportará no total 196 câmaras.

13. A AIPD apresentada apenas analisa os riscos do sistema relativos às novas 117 câmaras a instalar. Ora, uma avaliação de impacto dos riscos de um determinado tratamento de dados pessoais tem que considerar o sistema no seu todo, ou seja, no caso concreto, o processamento da informação decorrente das 196 câmaras, todo o *hardware* e *software*, bem como das infraestruturas a utilizar.

14. As imagens exemplificativas juntas ao pedido apresentam a aplicação de máscaras de privacidade nas tomadas de vista esperadas em cada uma das câmaras, sendo prestada informação que a PSP garantirá a

[1] Nos termos do disposto no artigo 29.º da Lei n.º 59/2019, de 8 de agosto, reiterado na alínea j) do n. º1 do artigo 6.º da Lei n.º 95/2021

aplicação de máscaras que protejam a privacidade dos cidadãos no momento da instalação (cf. Anexo B – Identificação do local e da área abrangidos pela captação).

15. Quanto às caraterísticas técnicas do equipamento a utilizar salienta-se que não são prestadas informações sobre mecanismos de "anti-tampering", isto é, meios de alerta em caso de tentativas de acesso não autorizado ou adulteração dos equipamentos, assim como sobre quaisquer mecanismos de proteção contra vandalismo, o que é essencial para que os equipamentos cumpram o exigido na alínea a) do ponto 2 do Anexo referido no artigo 2º da Portaria n.º 372/2012[2], de 16 de novembro (doravante apenas designada por Portaria).

16. Por outro lado, o sistema deverá permitir, e o responsável pelo tratamento deverá ter capacidade para, a alteração da chave de encriptação a cada seis meses, conforme exigido na alínea c) do ponto 3 do Anexo a que se refere o artigo 2.º da Portaria, o que não vem expresso na documentação apresentada.

17. Relativamente à encriptação das transmissões, apenas é mencionado o uso de TLS (*Transport Layer Security*). No entanto, nas características técnicas das câmaras há referência à versão 1.2, que, à data, é a versão que garante um nível de segurança mínimo. Na medida em que se está a projetar um sistema que, seguramente, até pelo investimento efetuado, será para perdurar, deverá garantir-se que a utilização da versão 1.3, atualmente recomendada por ser mais segura, o que garantirá um aumento significativo na segurança das comunicações;

18. É também mencionada, no Anexo F, junto ao pedido, a existência de uma proteção através de "*um codec MPEG-4 proprietário que será utilizado para proteger os fluxos de imagens transmitidos sobre a rede. Com esta medida, o vídeo intercetado poderá apenas ser visionado sobre o sistema onde corre a aplicação*". No entanto, o MPEG-4 é um padrão de compressão de áudio e vídeo que não tem documentada a característica de segurança referida. Assim, na ausência de mais informações sobre esse padrão/codec, não é possível verificar se esta medida cumpre efetivamente o propósito de proteção indicado ou se apenas se trata de uma medida de segurança por obscuridade[3]. Neste pressuposto, esta medida não atinge o seu objetivo porquanto um agente malicioso, com acesso à aplicação de visualização, pode descodificar, visualizar e exportar informação.

19. Quanto à arquitetura de comunicações, é afirmado que todos os equipamentos estarão conectados numa rede lógica privada (VPN), que, será segregada das restantes redes através de tecnologia *Multiprotocol Label Switching* e *Autonomously Provisioned Demands* (MPLS APD).

---

2 Aplicável nos termos do n.º 2 do artigo 145º do Código de Procedimento Administrativo.

3 Prática de ocultar detalhes de um sistema para melhorar a sua segurança, assumindo-se que essa falta de informação o protegerá de ataques.

20. A tecnologia *Trusted Platform Module* (TPM) impede o acesso de equipamentos não autorizados à gestão das câmaras. Contudo, não foi fornecida informação específica sobre outras medidas de isolamento e segregação das comunicações entre os dispositivos, sendo este tipo de medidas essencial para limitar outros vetores de ataque.

21. O pedido não fornece dados que permitam uma análise completa da arquitetura do sistema no que diz respeito à proveniência das credenciais de acesso. Embora na documentação se declare que "cada utilizador autorizado terá um perfil autónomo no servidor de vídeo, permitindo rastrear todas as ações realizadas no sistema", o que sugere que a base de dados de utilizadores está armazenada no servidor de vídeo, a alínea c) do artigo 3.º da Portaria é clara ao estipular que a autenticação deve ser realizada através da Rede Nacional de Segurança Interna (RNSI), e não diretamente no servidor de vídeo. Importa, por isso, corrigir esta situação.

22. Acresce que, quer na arquitetura apresentada, quer na documentação remetida, não há referência a uma ligação à RNSI, o que suscita dúvidas sobre o método e a proveniência da autenticação em uso.

23. No que diz respeito à hora legal portuguesa (em conformidade com o disposto no Artigo 4.º, número 2, alínea c), da Portaria) a AIPD menciona que "o servidor de vídeo está sincronizado com a hora legal, de forma a garantir a fidedignidade da data e hora que constarão em cada imagem captada, nas quais é igualmente indicado, de forma inequívoca, o local da captura". A partir desta afirmação, infere-se que, para assegurar a conformidade com a Portaria, o servidor de vídeo atua como servidor NTP (ou similar), garantindo que as câmaras captam e registam eventos sincronizados com a hora legal portuguesa. No entanto, uma vez que não está documentada qualquer ligação à Internet na infraestrutura, seria importante esclarecer qual a fonte utilizada para ajustar o servidor NTP e garantir assim a sincronização com a hora legal.

24. Quanto aos registos e auditorias (em conformidade com o disposto no Artigo 4.º, número 4 da Portaria), há a referir que não é indicada qual a política de retenção desses registos. É expectável que estes registos, que não devem conter dados pessoais, mas sim dados das operações realizadas, tenham um prazo de conservação significativamente superior aos 30 dias estipulados para a retenção das gravações. De outra forma, a sua finalidade ficaria esvaziada devido à dificuldade em permitir a deteção de padrões com uma amostragem tão reduzida ou a reconstrução de acessos e ações anómalas no sistema que tenham sido iniciadas há mais de 30 dias. Assim, à semelhança de outras situações, a CNPD recomenda a conservação dos registos de auditoria pelo prazo de 2 (dois) anos.

25. Dá-se ainda nota das exigências previstas no artigo 27.º da Lei n.º 59/2019, que são aplicáveis ao presente tratamento.

26. O pedido é omisso sobre a forma como a autenticidade e integridade desses registos são asseguradas. Idealmente, estes registos devem ser armazenados em ambientes independentes do servidor de vídeo, o que, de acordo com o descrito, não parece ser a arquitetura definida. Com efeito, manter o sistema a auditar junto com os registos de auditoria é uma prática que apresenta um risco significativo de comprometimento da integridade dos próprios registos. Um atacante que consiga acesso ao sistema de vídeo poderá, com mais facilidade, alterar ou eliminar os registos de auditoria, comprometendo assim a capacidade de detetar atividades ilícitas e violando a fiabilidade dos dados armazenados. Além disso, neste cenário, o administrador do sistema de vídeo pode também ter acesso aos registos de auditoria, o que não é desejável porquanto aumenta o risco de manipulação não autorizada, sem que tal seja possível detetar.

27. Na eventualidade de serem conservados no mesmo servidor, para mitigar o risco é essencial reforçar a necessidade de garantir que os operadores com privilégios de administração e os técnicos responsáveis pela manutenção do sistema não possam, em qualquer circunstância, obter acesso que lhes permita desligar ou modificar os registos de auditoria.

28. Não está documentado qualquer método de alarmística, o que é essencial do ponto de vista da prevenção e utilizações indevidas, criando padrões e identificação de situações típicas que permitirão a deteção precoce de anomalias do próprio sistema e de uso indevido.

III. Conclusão

29. Nos termos e com os fundamentos expostos a CNPD recomenda:

a. O equipamento a utilizar deve conter mecanismos de "anti-tampering", isto é, meios de alerta em caso de tentativas de acesso não autorizado ou adulteração dos equipamentos, e ainda mecanismos de proteção contra vandalismo, cumprindo, assim, o exigido na alínea a) do ponto 2 do Anexo referido no artigo 2º da Portaria n.º 372/2012, de 16 de novembro;

b. O sistema deverá permitir, e o responsável pelo tratamento deverá ter capacidade, para a alteração da chave de encriptação a cada seis meses, conforme exigido na alínea c) do ponto 3 do Anexo a que se refere o artigo 2.º da acima referida Portaria;

c. Relativamente à encriptação das transmissões, com o uso de TLS (*Transport Layer Security*), e porque se projeta um sistema para o futuro, deverá garantir-se a utilização da versão 1.3, que atualmente é recomendada por garantir um aumento significativo na segurança das comunicações;

d. Dos dados fornecidos infere-se que a base de dados de utilizadores está armazenada no servidor de vídeo. Contudo, a alínea c) do artigo 3.º da Portaria é clara ao estipular que a autenticação deve ser realizada através da Rede Nacional de Segurança Interna (RNSI), e não diretamente no servidor de vídeo, pelo que importa corrigir esta situação.

e. Quanto aos registos de auditorias que não devem conter dados pessoais, mas sim dados das operações realizadas, o prazo de conservação deve ser de 2 (dois) anos;

f. Guardar em local distinto os registos de auditoria, por forma a impedir o risco de comprometimento da integridade dos próprios registos;

g. A definição de métodos de alarmística, que tenham padrões e identifiquem situações típicas que permitirão a deteção precoce de anomalias do próprio sistema, assim como o seu uso indevido, para a prevenção de utilizações indevidas.

30. Dá-se nota que o pedido de Parecer remetido à CNPD incide apenas sobre o alargamento do sistema de videovigilância, ou seja, sobre 117 câmaras e não sobre o sistema na sua globalidade- como seria expectável por se tratar de um sistema único, que é composto por 196 câmaras e outros componentes, do qual as referidas 117 são apenas uma das partes integrantes.

Aprovado na reunião de 27 de agosto de 2024

Paula Meira Lourenço (Presidente)

Assinado por: **PAULA CRISTINA MEIRA LOURENÇO**
Data: 2024.08.27 20:50:34+01'00'
Certificado por: **Diário da República**
Atributos certificados: **Presidente - Comissão Nacional de Proteção de Dados**

CARTÃO DE CIDADÃO