CNPD
Comissão Nacional de Proteção de Dados

PARECER/2024/40

I. Pedido

1. O Secretário de Estado da Administração Interna solicitou parecer à Comissão Nacional de Proteção de Dados (CNPD) sobre o pedido de autorização do sistema de videovigilância na cidade de Ponta Delgada, Município de Ponta Delgada, que lhe foi submetido pela Polícia de Segurança Pública (PSP).

2. O referido pedido foi apresentado, nos termos do n.º 3 do artigo 5º, da Lei n.º 95/2021, de 29 de dezembro (doravante Lei n.º 95/2021), que regula a utilização e acesso pelas forças e serviços de segurança e pela Autoridade Nacional de Emergência e Proteção Civil a sistemas de videovigilância para captação, gravação e tratamento de imagem e som.

3. Pretende-se a instalação de um sistema de videovigilância constituído por 19 câmaras a operar de forma contínua, a instalar em diversos locais do Município de Ponta Delgada.

4. O pedido vem acompanhado de 10 anexos:

a. Fundamentos justificativos da necessidade e conveniência da instalação do sistema de videovigilância;

b. Identificação do local e da área abrangidos pela captação;

c. Identificação dos pontos de instalação das câmaras;

d. Características técnicas dos equipamentos utilizados;

e. Identificação do serviço responsável pela conservação e tratamento dos dados;

f. Procedimentos de informação ao público sobre a existência do sistema de videovigilância;

g. Mecanismos tendentes a assegurar o correto uso dos dados registados;

h. Comprovativo de garantia de financiamento da instalação do equipamento utilizado e das respetivas despesas de manutenção.

i. Avaliação de impacto do tratamento de dados sobre a proteção de dados pessoais, prevista no artigo 29.º da Lei n.º 59/2019.

j. Protocolo de cooperação entre o Município de Ponta Delgada e a PSP relativo à implementação de um sistema de videovigilância a instalar na cidade de Ponta Delgada

5. Não consta da documentação recebida o contrato de aquisição do sistema de videovigilância realizado pela Câmara Municipal, que inclui a manutenção do sistema, a reparação e a substituição dos equipamentos avariados, informação que não foi possível recolher através da consulta do Portal Base.

I. Apreciação

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

6. A CNPD emite parecer nos termos do n.º 3 e no prazo fixado pelo n.º 4 do artigo 5.º da Lei n.º 95/2021, em conjugação com as alíneas b) e c) do artigo 87.º do Código do Procedimento Administrativo.

7. A pronúncia da CNPD restringe-se à apreciação da conformidade do pedido apresentado com a observância das regras referentes à 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 da Lei n.º 95/2021.

8. É, por isso, também objeto de parecer da CNPD, de acordo com as referidas normas, 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 dos cidadãos.

9. 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.

10. 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.

ii. Do tratamento decorrente da videovigilância no Município de Ponta Delgada

11. Em causa está um tratamento de dados decorrente do pedido de autorização de instalação de um sistema de videovigilância no Município de Ponta Delgada, constituído por 19 câmaras.

12. O anexo B apresenta imagens da zona que será abrangida por cada uma das câmaras.

13. Desde logo, as imagens apresentadas foram captadas a uma altura substancialmente inferior aos 4 metros referidos na documentação para a sua localização final, o que não é irrelevante do ponto de vista de proteção de dados.

14. O envio à CNPD das imagens que serão abrangidos pelas captações serve precisamente para que esta se possa pronunciar sobre a utilização de câmaras em áreas que sejam, pela sua natureza, destinadas a ser utilizadas em resguardo, bem como a instalação e utilização de câmaras quando a captação de imagens e de sons abranja afete a esfera da reserva da vida privada dos cidadãos.

15. Apesar de ser afirmado que "serão colocadas máscaras em todos os locais onde deve ser preservada a privacidade, designadamente, janelas, varandas e portas de edifícios de habitação, edifícios hoteleiros ou similares", as máscaras não foram aplicadas nas imagens exemplificativas juntas.

16. Era ainda pressuposto que as imagens juntas ao pedido apresentassem a aplicação de máscaras de privacidade nas tomadas de vistas esperadas em cada uma das câmaras. Temos assim apenas a afirmação, sem fornecer dados à CNPD que lhe permitam pronunciar-se.

17. No que respeita às caraterísticas técnicas das câmaras e dos equipamentos é afirmado que quanto aos microfones "este recurso não será utilizado e será bloqueado nativamente na instalação através da chave de segurança licenciada".

18. Não foram disponibilizadas as características técnicas das câmaras e dos equipamentos, mas da afirmação constante no Anexo D resulta que o sistema dispõe de microfones, logo tem capacidade para a recolha de som e que a funcionalidade de captação será desabilitada.

19. Sem conhecer o modelo das câmaras e a configuração do sistema, a CNPD não pode garantir que o bloqueio é eficaz, designadamente se um utilizador com poderes de administração pode alterar essa configuração e se tal alteração fica refletida nos registos de auditoria.

20. Também quanto às caraterísticas técnicas do equipamento a utilizar não foram facultados elementos relevantes. Não é disponibilizada informação sobre meios de alerta em caso de tentativas de acesso não autorizado ou de adulteração dos equipamento, assim como sobre a existência de mecanismos de proteção contra o vandalismo (anti-*tampering*), desconhecendo-se, por isso, se os equipamentos cumprem o exigido na

alínea a) do ponto 2 do Anexo referido no artigo 2º da Portaria n.º 372/2012[1], de 16 de novembro (doravante Portaria).

21. Omissa está também informação sobre a capacidade de o responsável pelo tratamento alterar a chave de encriptação a cada seis meses, como prescreve a alínea c) do ponto 3 do Anexo a que se refere o artigo 2.º da Portaria

22. No que respeita à encriptação das transmissões, apenas é mencionado o uso de TLS (*Transport Layer Security*), sem, contudo, se indicar a versão do mesmo, o que inviabiliza a pronúncia sobre se se mostra respeitado o disposto na alínea c) do ponto 3 do Anexo da referida Portaria.

23. Afirma-se nos Anexos G e I a existência de uma proteção através de "um codec MPEG-4, 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".

24. 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[2]. Neste pressuposto, sempre se dirá que esta medida não atinge o seu objetivo porquanto um agente malicioso, com acesso à aplicação de visualização, pode descodificar, visualizar e exportar informação.

25. Nada se refere no pedido sobre o sistema de gestão analítica dos dados captados, não estando referenciado qualquer tipo de analítica, situação que nos parece estranha face à realidade atual destes sistemas,

26. No que toca aos mecanismos tendentes a assegurar o correto uso dos dados registados, são fornecidas informações sobre a segurança física do centro de dados e do centro de operações, locais guardados 24 horas por dia e com controlo de acesso por código. As medidas implementadas para controlo de acesso ao Centro de Comando e Controlo Operacional, bem como os procedimentos para acesso por pessoal não credenciado são adequadas. No entanto, não são prestadas informações relativas à infraestrutura que conecta as câmaras

---

[1] Portaria aplicável nos termos do n.º 2 do artigo 145º do Código de Procedimento Administrativo.

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

ao centro de dados, designadamente, não existe informação em que tipo de armários se encontram instaladas as caixas de passagem e distribuição onde se encontram instalados, por exemplo, "os switches de outdoor, de calibre industrial".

27. Também nada se refere à cablagem, nomeadamente sobre se o percurso será realizado através de tubagem subterrânea e inacessível ou através de cabos expostos e de fácil acesso.

28. Salienta-se ainda que, quer na arquitetura apresentada, quer na documentação remetida, não há referência a ligação à Rede Nacional de Segurança Interna, o que suscita dúvidas sobre o método e a proveniência da autenticação em uso.

29. Quanto à arquitetura de comunicações, por ausência de informação não se mostra possível realizar qualquer análise.

30. Relativamente aos perfis de acesso ao sistema (cf. artigo 3º da Portaria) , retira-se da informação constante do Anexo G que o acesso ao sistema é feito através de autenticação por utilizador e palavra-passe e está circunscrito a agentes da PSP formados e credenciados para essas funções.

31. Mas, o pedido não fornece outros 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 operador terá um perfil autónomo no servidor de vídeo", o que sugere que a base de dados de utilizadores estará 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. Acresce que

32. 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". 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.

33. Quanto aos registos e auditorias (em conformidade com o disposto no Artigo 4.º, número 4 da Portaria), há a referir que é mencionada a existência de mecanismos de registo e auditoria, sendo os registos conservados por um período de seis meses.

34. É expectável que estes registos tenham um prazo de conservação adequado para permitir a deteção de padrões ou a reconstrução de acessos e ações anómalas, sob pena de a sua finalidade ficar esvaziada, pelo que, à semelhança de outras situações, a CNPD recomenda a conservação dos registos de auditoria pelo prazo de 2 (dois) anos.

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

36. 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.

37. 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.

38. Apesar de serem identificados cenários capazes de gerar registos, 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.

39. Com base nos registos previstos e de todos os que forem considerados necessários para a deteção precoce de anomalias e usos indevidos, devem ser gerados alertas que, consoante o tipo e gravidade, devem ser recebidos e objeto de análise por uma pessoa ou equipa especificamente designada para desempenhar essa função e ser adotada uma Política de Gestão de Incidentes.

II. Conclusão

Nos termos e com os fundamentos expostos, que tiveram por base as informações prestadas e analisadas, a CNPD recomenda:

i. A colocação de máscaras em todos os locais onde deve ser preservada a privacidade, designadamente, janelas, varandas e portas de edifícios de habitação, edifícios hoteleiros ou similares;

ii. O sistema deve conter mecanismos de alerta em caso de tentativas de acesso não autorizado ou adulteração dos equipamentos, e ainda mecanismos de proteção contra vandalismo;

iii. A proteção dos fluxos de imagens transmitidos sobre a rede através de um *codec* MPEG-A que efetivamente impeça que as imagens possam ser visionadas noutro sistema que não aquele em que corre a aplicação;

iv. O sistema deverá permitir, e o responsável pelo tratamento deverá ter capacidade, para a alteração da chave de encriptação a cada seis meses;

v. Que a autenticação dos utilizadores seja realizada através da Rede Nacional de Segurança Interna (RNSI), e não diretamente no servidor de vídeo;

vi. Os registos de autoria devem ser configurados por forma a registarem qualquer alteração que venha a ser introduzida no sistema, ainda que efetuada por utilizadores com poderes de administração;

vii. Estes registos devem ser conservados pelo prazo de 2 (dois) anos e guardados em local distinto, por forma a impedir o risco de comprometimento da sua integridade;

viii. 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.

Aprovado na reunião de 15 de outubro de 2024

Luís Barroso (Vogal em substituição da Presidente)