INSTITUTO SUPERIOR DE CIÊNCIAS POLICIAIS E SEGURANÇA INTERNA

VI CURSO DE COMANDO E DIREÇÃO POLICIAL

Trabalho Individual Final

Videovigilância na via pública: o responsável pelo tratamento de dados na PSP

Auditor

Fábio Miguel Dionísio Martins

Comissário M/152501

Lisboa, 03 de outubro de 2025

RESUMO

A videovigilância na via pública implementada nos últimos anos em Portugal demonstra ser uma ferramenta extremamente útil na prossecução da segurança, com a sua utilização sempre em conformidade com o quadro jurídico nacional. Apesar da sua aplicabilidade nas atribuições da PSP, o seu uso tem um elevado impacto nos direitos e liberdades (direito à privacidade e imagem), bem como apresenta um risco no tratamento dos dados pessoais das pessoas que sejam captados pelo sistema. Para o tratamento desses dados e garantia da conformidade e confidencialidade dos dados pessoais é necessário que sejam adotadas medidas técnicas e organizativas que respondam às exigências da proteção e respeito pelos direitos dos particulares, nomeadamente na garantia da segurança do tratamento dos dados pessoais através do conhecimento de quais as medidas necessárias, bem como das responsabilidades e funções inerentes ao papel de Responsável pelo Tratamento de dados nomeado. Estas atribuições e funções têm como final esperado a inexistência de violações e incidentes no tratamento, garantindo igualmente que os dados tratados estão a ser utilizados para o fim previsto na lei.

Palavras-chave: espaços públicos, dados pessoais, medidas de segurança, responsável pelo tratamento, videovigilância

ABSTRACT

Video surveillance on public roads implemented in recent years in Portugal has proven to be an extremely useful tool in pursuing security, with its use always in accordance with the national legal framework. Despite its applicability in the duties of the PSP, its use has a high impact on rights and freedoms (right to privacy and image), as well as presenting a risk in the processing of personal data of people who are recorded by the system. In order to process this data and ensure compliance and confidentiality, it is necessary to adopt technical and organizational measures that meet the requirements of protection and respect for the rights of individuals, namely by ensuring the security of personal data processing through knowledge of the necessary measures, as well as the responsibilities and functions inherent to the role of the appointed Data Controller. The expected outcome of these duties and functions is the absence of breaches and incidents in the processing, while also ensuring that the data processed is being used for the purpose provided by law.

Keywords: video surveillance, public space, security measures, personal data, data controller

ÍNDICE

INTRODUÇÃO

O fenómeno da utilização em larga escala de sistemas de videovigilância na via pública é um facto e como tal as sociedades têm sentido a dicotomia da segurança *versus* liberdade, de uma forma mais agudizada no seu quotidiano.

Existe uma tensão na necessidade de conciliar a segurança, enquanto função essencial que legitima a existência do Estado (Inácio, 2018), com o direito à liberdade e à segurança de todos, consagrado constitucionalmente (Canotilho e Moreira, 2008; Pereira, 2017). A segurança é inerentemente considerada o garante do exercício da liberdade (Moreira, 2013). Contudo, com a aplicação de medidas de vigilância eletrónica e mais concretamente a videovigilância no espaço público, esta é vista como uma ameaça à liberdade individual, levantando questões sobre o controlo da via pública (Frois, 2011).

A adoção deste tipo de tecnologia é sustentada por uma estratégia que, por vezes, se socorre de um discurso de videoproteção (Rodrigues, 2024 e Melo & Viseu, 2024), visando invocar a mentalidade de que o Estado protege os seus cidadãos, enquanto afasta a perceção da lógica disciplinar (Foucault, 1987).

Contudo, o Estado tem a obrigação constitucional de garantir a segurança (*cf.* al. b) e d) do artigo 9.º e 27.º da Constituição da República Portuguesa, bem como mais especificamente no que tange às funções de polícia, o estipulado no artigo 272.º). Neste contexto, e com a utilização da tecnologia como suporte da atividade policial, surge a necessidade de promover a salvaguarda e tratamento de dados pessoais, que, eventualmente, possam ser captados pelos sistemas de videovigilância na via pública em uso pelas forças e serviços de segurança, e a garantia da legalidade da sua ação policial, garantido desta forma que as ações das polícias se pautam pela estrita observância das regras do Estado de Direito Social (Inácio, 2018).

É neste contexto — em que se impõe a proteção dos dados pessoais tratados nos diversos sistemas de videovigilância em uso pelas forças e serviços de segurança em Portugal — que nos propomos desenvolver o presente estudo, de acordo com a observância dos Direitos, Liberdades e Garantias constitucionalmente consagrados em conjugação com as atribuições e responsabilidades do Responsável pelo Tratamento de Dados (RTD) dos sistemas de videovigilância na via pública em utilização pela Polícia de Segurança Publica (PSP), à luz do quadro jurídico atualmente em vigor.

Pertinência e justificação da escolha do tema

Usualmente as atividades de investigação sobre videovigilância e sistemas de videovigilância na via pública, incidem sobre os resultados operacionais da prevenção criminal e reação a crimes ocorridos em áreas vigiadas (Pereira, 2017), bem como a metodologia da organização processual de pedidos de autorização ao Ministério da Administração Interna (Rodrigues, 2024; Frias, 2024). Contudo, verificámos, após análise às normas internas da PSP e estudos de investigação, que existe um vazio investigatório sobre o papel do RTD, interveniente com especial relevo em todo o processo de tramitação no tratamento de dados dos sistemas de videovigilância na via pública.

Após uma análise sobre o estado da arte, bem como a demonstração da realidade existente no seio da PSP, é intenção que o presente estudo traga uma mais valia para o funcionamento e operação dos sistemas, uma vez que possibilitará demonstrar a opinião e as necessidades de quem trabalha efetivamente com este tipo de equipamentos, bem como irá possibilitar o avanço na metodologia e nos processos inerentes ao tratamento e segurança dos dados pessoais.

Delimitação do objeto de estudo

No que diz respeito ao objeto de estudo, e tendo em conta que a literatura académica dedica escassa atenção ao papel e às responsabilidades do RTD, afigura-se como pertinente proceder a uma avaliação e à descrição das medidas de segurança (quer no domínio físico, quer no informático). Não se pretende, porém, avaliar a qualidade dos processos instrutórios nem mesmo analisar as necessidades legislativas nacionais, mas antes centrar-nos exclusivamente nas funções e responsabilidades do RTD na PSP.

Metodologia

No que concerne à metodologia adotada para a consecução dos objetivos delineados, este estudo assenta numa abordagem de carácter misto, articulando uma dimensão teórica-dogmática com uma componente empírica. A primeira fase de investigação será conduzida através de uma metodologia qualitativa de natureza bibliográfica e documental. Proceder-se-á a uma análise crítica e sistemática do estado da arte, através da doutrina académica nacional e internacional, da jurisprudência relevante e do quadro legal aplicável, com especial enfoque na legislação de proteção de dados e nos normativos internos da PSP. Esta

etapa permitirá construir um robusto enquadramento teórico, sistematizando o regime jurídico do RTD e fundamentando a definição das suas funções, responsabilidades e perfil, respondendo assim aos primeiros objetivos da pesquisa.

Para densificar e validar os achados teóricos, bem como para explorar as hipóteses de trabalho colocadas, o estudo integrará uma componente empírica de natureza quantitativa. Esta será operacionalizada através da realização de entrevistas semi-estruturadas, aplicadas sob a forma de questionário online aos Chefes da Àrea Operacional dos comandos da PSP, ou de quem esteja a desempenhar as funções de RTD, com sistemas de videovigilância implementados. A opção por este instrumento permitirá recolher, de forma sistemática e passível de análise estatística, a perceção, as experiências concretas e as necessidades identificadas pelos profissionais que efetivamente desempenham ou supervisionam as atividades de tratamento de dados.

Com a integração destes dois métodos procuramos produzir uma análise compreensiva que, para além de sistematizar o enquadramento legal e doutrinário, permita identificar lacunas, constrangimentos e necessidades sentidas pelos RTD. Assim, a metodologia adoptada possibilita não apenas uma descrição rigorosa e assertiva do papel e das responsabilidades destes profissionais, mas também a formulação de recomendações fundamentadas para o aperfeiçoamento dos processos internos da PSP em matéria de tratamento de dados pessoais no contexto da videovigilância.

Definição do Problema e dos Objetivos de Investigação

Relativamente às hipóteses em causa com este estudo, definimos da seguinte forma:

i. saberão os RTD nomeados as suas funções e responsabilidades.
ii. os RTD têm à sua disposição as ferramentas necessárias para o bom desempenho das suas funções e responsabilidades.
iii. que necessidades sentem os RTD quando estão no desempenho das funções.

Colocam-se os seguintes objetivos a atingir com o presente estudo:

i. Analisar e sistematizar o enquadramento legal aplicável à videovigilância na via pública e ao RTD em sistemas de videovigilância da PSP;
ii. Definir as funções, responsabilidades e perfil de competências do RTD na PSP;
iii. Desenvolver recomendações/melhorias para a criação de um protocolo interno de atuação e *accountability* nas funções do RTD.

ESTADO DE ARTE

A videovigilância na via pública, no rigor que o tema implica, é um tema complexo e abrangente, que agrega simultaneamente a vertente tecnológica de controlo, a vertente de proteção de dados pessoais e a vertente de ferramenta no âmbito das políticas públicas de prevenção criminal, conforme define Rodrigues (2024), em que as forças de segurança, e em concreto a PSP poderá utilizar como instrumento de apoio à atividade operacional.

Para a análise do panorama nacional é importante destacar o facto de em Portugal a massificação do uso e dos pedidos de autorização de instalação apenas aconteceu nos últimos cinco anos, apesar de contar com legislação que regula o uso de câmaras de videovigilância na via pública há sensivelmente vinte anos, permitindo que neste momento ainda nos encontremos numa fase de "descoberta" e de conhecimento das potencialidades, bem como dos riscos e responsabilidades do uso de um meio de vigilância tão intrusivo nos direitos, liberdades e garantias individuais.

Videovigilância na via pública – enquadramento nacional

Em Portugal, segundo Melo e Viseu (2024) a utilização de videovigilância na via pública foi sempre caracterizada por uma tensão histórica e sociopolítica entre a necessidade de segurança e a salvaguarda dos direitos fundamentais, nomeadamente a privacidade e a proteção de dados pessoais.

Apesar de existir esta indecisão quanto à vertente que deverá prevalecer, se for analisada a utilização e os usos da videovigilância nos espaços públicos portugueses revela uma evolução marcada por fases distintas, definidas pela alteração do quadro legal, conforme descreve Melo e Viseu (2024) – a fase restritiva- experimental e a consolidação expansionista, ou mesmo por três fases de acordo com Moreira (2013) – a fase experimental, a restritiva-experimental e a fase expansionista.

Neste quadro de mutação da legislação ao longo do tempo, poderemos apontar como o surgimento da primeira legislação nacional, que permitiu a utilização de meios de vigilância eletrónica, a publicação da Lei Orgânica n.º 2/2004, de 12 de maio, por ocasião da realização do Campeonato Europeu de Futebol – Euro 2004 (Moreira, 2013; Pereira, 2019).

Na sequência desta fase experimental, surge em Portugal a primeira lei que estabeleceu o regime definitivo para a utilização de câmaras pelas forças e serviços de

segurança em locais públicas – a Lei n.º 1/2005, de 10 de janeiro. Esta primeira lei, de acordo com Melo e Viseu (2024), é caracterizada por se apresentar como uma legislação restritiva, vincada pelo primado do direito à privacidade, com um forte poder da Comissão Nacional de Proteção de Dados (CNPD) através do seu parecer vinculativo.

No período de 2005 a 2012, resultado desta forte pressão da garantia da privacidade e da falta de argumentos válidos e objetividade da sua necessidade (Rodrigues, 2024), o número de sistemas autorizados e instalados foi praticamente nulo.

Foi com a alteração introduzida pela Lei n.º 9/2012, de 23 de fevereiro, que veio retirar a força vinculativa ao parecer emanado pela CNPD (n.º 2 do artigo 3.º da Lei n.º 9/2012) e restringindo a sua pronúncia à segurança do tratamento e conservação dos dados pessoais, que se iniciou uma nova fase no que reporta à autorização de instalação e funcionamento de sistemas de videovigilância. Neste seguimento surge igualmente a primeira, e única, regulamentação neste âmbito, com a publicação da Portaria n.º 372/2012, de 12 de novembro (requisitos técnicos das câmaras) e da Portaria n.º 373/2012, de 16 de novembro (modelos de avisos e simbologia da utilização de câmaras). Com esta alteração, surgiu então a primeira grande oportunidade de as forças de segurança promoverem a instrução de processos e submetê-los ao Ministério da Administração Interna para autorização.

Em 2021, e após um período de imenso debate sobre a adequabilidade do enquadramento jurídico dos sistemas de videovigilância na via pública, foi publicada a Lei n.º 95/2021, de 29 de dezembro, que veio regular a utilização e o 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, revogando a Lei n.º 1/2005, de 10 de janeiro, com a definição clara e objetiva dos fins para que os sistemas os sistemas podem ser usados (artigo 3.º da Lei n.º 95/2021).

A entrada em vigor Lei n.º 95/2021 marca a fase expansionista em Portugal por vir definir e consolidar o regime jurídico da videovigilância, introduzindo inovações significativas no âmbito da recolha e tratamento de dados. Estas regras específicas incluem, entre outras, a possibilidade de utilização de uma gestão analítica de vídeo (n.º 1 do artigo 16.º da Lei n.º 95/2021), necessidade de realização de uma avaliação de impacto do tratamento de dados (al. j) do n.º 1 do artigo 6.º da Lei n.º 95/2021, bem como definição da responsabilidade do tratamento, regendo-se pela Lei n.º 59/2019, extensiva aos contratos

celebrados com terceiros (subcontratação), sendo necessário formalizar contratualmente a relação de subcontratação nos termos do artigo 23.º da Lei n.º 59/2019.

Quanto ao emprego da Lei n.º 95/2021, a mesma está subjacente à aplicação de princípios norteadores da sua utilização, tais como a proporcionalidade, adequação, necessidade e legalidade (artigo 7.º).

Como não poderia deixar de ser, importa ainda realçar que o regime jurídico português relativo à videovigilância em espaços públicos, Lei n.º 95/2021, está intrinsecamente ligado a um quadro legal multinível, onde se inclui o Regulamento Geral de Proteção de Dados (RGPD), o Regulamento (UE) 2016/680, e as respetivas leis nacionais de execução, a Lei n.º 58/2019 e a Lei n.º 59/2019, respetivamente.

O responsável pelo tratamento de dados pessoais

A aplicação do regime jurídico de sistemas de videovigilância na via pública implica um quadro legal complexo de proteção de dados. Neste contexto, o RTD assume um papel fulcral para a garantia da conformidade legal, técnica e organizacional do tratamento de dados (CNPD, 2023a).

De acordo com os artigos 20.º e seguintes da Lei n.º 59/2019, o RTD é definido como a entidade competente que, individualmente ou em conjunto com outras determina as finalidades e os meios de tratamento dos dados pessoais, com o especial dever de responsabilidade, ou seja, deve assegurar e comprovar que o tratamento dos dados pessoais é realizado em conformidade com os princípios legais (CNPD, 2023a; Lei n.º 59/2019; Diretiva (UE) 2016/680). No caso em estudo, especificamente na PSP, este tratamento regulado pela Lei n.º 95/2021, em tudo que não esteja especificamente previsto na referida lei, rege-se pelo disposto na Lei n.º 59/2019.

Este ponto é verdadeiramente importante por excluir o RGPD, dado que não é aplicável o tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção e repressão de infrações penais e salvaguarda da segurança pública (Frias, 2024, Diretiva (UE) 2016/680).

No que tange ao RTD, cumpre destacar as suas responsabilidades no tratamento e segurança dos dados, onde se incluem as obrigações previstas pela Lei n.º 59/2019 e reforçadas pela Lei n.º 95/2021. Especificamente o RTD, no âmbito do tratamento dados por sistemas de videovigilância na via pública operados pela PSP, tem como responsabilidade a realização de uma avaliação de impacto sobre a proteção de dados – AIPD (artigo 29.º da

Lei 59/2019 e artigo 27.º da Diretiva (UE) 2016/680), garantir a confidencialidade, a segurança e a integridade dos dados através da adoção de medidas técnicas e organizativas apropriadas para assegurar um nível de segurança adequado ao risco (CNP, 2023a), garantir o registo das atividades de tratamento, bem como os registos de auditoria (artigo 26.º da Lei n.º 59/2019), notificação à autoridade de controlo, CNPD, de violação de dados pessoais, e em caso dessa violação implicar um elevado risco para os direitos e liberdades, notificar os titulares dos dados (CNPD, 2023a) e garantir que a subcontratação é regulada mantendo o ónus do tratamento dos dados pessoais no RTD (artigo 23.º da Lei n.º 59/2019).

Pelo exposto, verifica-se que o RTD tem sob sua alçada uma panóplia de responsabilidades inerentes à sua função na garantia do correto tratamento de dados, com a aplicação das medidas técnicas e organizativas necessárias, incluindo através da subcontratação.

Direitos e deveres dos titulares dos dados pessoais

A Lei n.º 95/2021 consagra, por remissão à demais legislação que rege os dados pessoais, um conjunto de direitos fundamentais aos titulares dos dados, bem como impõe obrigações processuais para o exercício desses direitos, bem como deveres.

Antes de densificarmos quais são esses direitos e deveres, importa definir de acordo n.º 1 do artigo 3.º da Diretiva (UE) 2016/680:

> «Dados pessoais», informações relativas a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador como, por exemplo, um nome, um número de identificação, dados de localização, identificadores em linha ou um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular.

Nestes termos, podemos enunciar com maior rigor que ao titular dos dados pessoais assiste a faculdade de solicitar o direito de acesso e informação junto do RTD, para confirmação de que os dados pessoais que lhe dizem respeito estão ou não a ser objeto de tratamento (artigo 15.º da Lei n.º 59/2019), devendo o RTD disponibilizar as informações solicitadas (artigo 13.º da Lei n.º 59/2019), o direito de retificação ou apagamento dos dados

pessoais e de limitação do tratamento (artigo 17.º da Lei n.º 59/2019) e direito de apresentar queixa à autoridade de controlo (artigo 47.º da Lei n.º 59/2019).

Embora a legislação se concentre nos direitos dos titulares e nas obrigações do RTD, para que os direitos possam ser exercidos é exigido que se cumpram alguns deveres, tais como o dever de não abuso de direito através de pedidos manifestamente infundados ou excessivos (n.º 5 do artigo 13.º da Lei n.º 59/2019).

No regime jurídico em análise para o estudo, em concreto no definido nos artigos 16.º e 17.º da Lei n.º 59/2019 e no artigo 20.º da Lei n.º 95/2021, importa ainda destacar a possibilidade do RTD fundamentadamente recusar o exercício do direito de acesso e eliminação ao titular dos dados.

Verifica-se, pois, uma estreita ligação entre o exercício dos direitos do titular dos dados e as funções e responsabilidades do RTD, para um tratamento correto, lícito e transparente, assegurado pela integridade e confidencialidade dos dados.

MEDIDAS DE PROTEÇÃO DOS DADOS PESSOAIS

A segurança do tratamento de dados pessoais constitui um pilar fundamental nas funções do RTD, de acordo com o quadro normativo, designadamente o Regulamento (UE) 2016/679, do Parlamento Europeu e do Conselho, de 27 de abril de 2016 (doravante designado por Regulamento Geral sobre a Proteção de Dados – RGPD). O RTD detém em si a obrigação e responsabilidade de assegurar a conformidade e a devida proteção dos dados e dos direitos dos titulares. Nesta base, a CNPD enquanto autoridade de controlo, na prossecução definida na alínea d) do n.º 1 do artigo 57.º do RGPD, em conjugação com o artigo 3.º da Lei n.º 58/2019, entende que deverão ser definidos e clarificados quais as obrigações no domínio da segurança dos dados pessoais (CNPD, 2023a) sob responsabilidade do RTD. Deste modo, é essencial analisar que medidas de segurança e proteção dos dados pessoais podem ser concretizadas durante o tratamento de dados na operação dos sistemas de videovigilância.

Medidas de segurança física

Tendo em conta que nos propomos analisar o papel do RTD no âmbito da instalação e funcionamento de sistemas de videovigilância na via pública, torna-se imperativo examinar as medidas de proteção dos dados pessoais passíveis de implementação obrigatória e sobre

responsabilidade do RTD. Nesta primeira análise às medidas de proteção, incidiremos com especial destaque para as medidas de segurança física, enquanto componente fundamental da proteção e garantia da inviolabilidade dos dados pessoais.

Este tipo de segurança consiste na aplicação de medidas físicas, técnicas e procedimentais de proteção, que visam impedir o acesso não autorizado a informações sensíveis, nas quais se incluem os dados pessoais (GNS, 2018). A sua atuação deve focar-se na salvaguarda dos profissionais, bem como na prevenção de acessos não autorizados a informações, materiais e instalações (SEGNAC 1). Refere ainda o GNS (2018) que as medidas devem ser implementadas em todas as instalações, edifícios, gabinetes, salas técnicas ou outras zonas onde se armazenem/manuseiem dados pessoais, incluindo os locais onde se encontram as redes e os sistemas de informação que processam os dados.

Na fase de implementação, define a SEGNAC 1 que existe a necessidade de promover um estudo das ameaças como requisito técnico e organizacional, através de uma avaliação informada do cenário de risco, de forma que as medidas implementadas sejam adequadas e proporcionais ao risco identificado.

Após esta análise/avaliação, poderemos identificar a implementação das medidas através de uma estratégia de defesa em profundidade, com medidas em múltiplos níveis com o objetivo de proteger e impedir o acesso não autorizado, detetar acessos ou tentativas de acesso e retardar os intrusos para que exista uma ação da autoridade competente (GNS, 2018).

No diz respeito a medidas organizativas de controlo de acessos, deverá ser instituído um processo de credenciação de pessoas através de um salvo-conduto (cartão de acesso ou dados biométricos) para o pessoal permanente (SEGNAC 2), em que os visitantes deverão ter autorização prévia e específica e ser acompanhados permanentemente, com um registo de entradas de pessoas não autorizadas por um período de 12 meses (GNS, 2018). As medidas implementadas deverão também abranger a segurança das instalações, com iluminação adequada, sistemas eletrónicos de vigilância, portas de acesso sólidas e com controlos de acesso (biométrico ou cartão/senha individual) (GNS, 2018) garantindo desta forma que o acesso só é possível a tem a necessidade aceder aos dados.

Todos estas medidas deverão ser revistas periodicamente (existindo capacidade, anualmente) e realizada nova avaliação pelo RTD, como garantia da atualidade e premência da carência de implementação de medidas de segurança inerentes aos riscos detetados.

Medidas de segurança informáticas

Relativamente às medidas de segurança informática, importa destacar que é uma área de desenvolvimento do conhecimento muito rápido, o que leva a que exista uma avaliação substantiva e profunda das operações de tratamento e potenciais riscos envolvidos.

Nestes moldes, para que se possam implementar ações efetivas, é necessário que se promova uma mentalidade que envolva a aplicação de medidas organizativas, com procedimentos e políticas internas, que adaptem a instituição na gestão da segurança da informação e a proteção de dados (CNPD, 2023a). Refere ainda a CNPD (2023a) que é indispensável a definição de um planeamento e gestão dos incidentes, com exercícios práticos de resposta a incidentes e recuperação de desastres, diligenciando para a resiliência dos sistemas.

Outro ponto primordial das medidas organizativas a implementar será a gestão de acessos e perfis nos diversos intervenientes/operadores do sistema (CNCS, 2019), com a definição de uma política de gestão de palavras-passe seguras, em que são atribuídos perfis de acesso condicionado ao princípio da necessidade de conhecer e com as permissões de acesso e as autorizações de acordo com os princípios de menor privilégio e de segregação de funções, com uma política de gestão de acessos lógicos e físicos (CNPD, 2023a).

Relativamente às auditorias e reavaliações, cabe ao RTD realizar e manter registo de todas as auditorias executadas por um período de 2 anos (PSP, 2024), incluindo a realização de avaliações de vulnerabilidades para identificar fragilidades e orientar formação específica se assim for necessário. Nas medidas de segurança implementadas, incluindo as dos subcontratantes, deverá ser verificado se mantêm a sua validade e eficácia, diligenciando por atualizações regulares, com as vulnerabilidades detetadas a serem documentadas e corrigidas no mais curto espaço de tempo (CNPD, 2023a).

Para além das medidas mencionadas, realça-se que toda a infraestrutura mantenha uma organização que permita a segmentação ou isolamento das redes de dados para prevenção de possíveis ataques por *malware*, bem como deverão manter atualizados os sistemas operativos (nos servidores e terminais) e de todas as aplicações, bem como o *firmware* dos equipamentos de rede (CNPD, 2023a).

Na resiliência contra ameaças, refere ainda a CNPD (2023a) que é dever da organização, entenda-se do RTD, implementar ferramentas *antimalware* que permitam a deteção, verificação e bloqueio em tempo real de ameaças, tais como o *ransomware.* Como tal, deverá estar em vigor um sistema de cópia de segurança (*backup*), seguro e testado,

separado dos servidores operacionais e sem acessibilidade externa, para resiliência em caso de incidente (CNCS, 2019; CNPD, 2023a).

Outro aspeto que poderá ser implementado, conforme descreve o CNCS (2019), é a utilização de alarmística que permita a identificação de situações de acesso, tentativa ou utilização indevida, para monitorização constante da rede, dos sistemas de informação e mesmo do ambiente físico contra potenciais incidentes de segurança, bem como a monitorização das atividades de todos os operadores do sistema.

Por último, chama-se à colação o Regulamento (UE) 2024/2847 do Parlamento Europeu e do Conselho, de 23 de outubro de 2024 (Regulamento de Ciber-Resiliência), o qual vem reforçar as obrigações do RTD ao exigir que os produtos sejam disponibilizados sem vulnerabilidades conhecidas e com uma configuração segura por defeito, protejam a confidencialidade dos dados pessoais, tratem apenas os dados necessários/autorizados, assegurem a disponibilidade de funções essenciais, mesmo após um incidente e tenham uma política e mecanismos de tratamento eficaz.

Pelo exposto, entende-se que as funções e responsabilidades do RTD vão muito mais além da auditoria e avaliação aos sistemas implementados, alcançando todas as vertentes da segurança e resiliência informáticas necessárias, tal como a definição de perfis e acessos, *software* e confidencialidade dos dados pessoais, numa metodologia contínua de evolução, definida pelo CNCS (2019) em cinco funções: identificar, proteger, detetar, responder e recuperar.

Aplicabilidade da Norma ISO/IEC 2700:2022 e da Diretiva NIS2

No desempenho das funções de RTD e na garantia da segurança da informação, existem diversas ferramentas que poderão auxiliar e melhorar a capacidade de resiliência a riscos, bem como facilitar a operação e introdução de procedimentos concretos e conhecidos de todos os operadores para a garantia da inviolabilidade no tratamento dos dados pessoais nos sistemas de videovigilância.

Nesta conjuntura, verifica-se que existem normas e procedimentos que já demonstraram a sua adequabilidade ao que se propõe, nomeadamente a aplicação da Norma ISO/IEC 27001:2022, através do qual se especificam os requisitos formais para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão de segurança da informação (SGSI) no contexto de uma organização.

No caso concreto, e verificando o contexto da PSP, para a aplicação da ISO/IEC 27001 à videovigilância na via pública, passaria pela obrigatoriedade de criação de um SGSI que abranja todo o ciclo de vida das imagens: recolha, transmissão, armazenamento, consulta e destruição.

Com a aplicação da Norma ISO/IEC 27001:2022 e a com a criação deste SGSI surge a necessidade de reforço do cumprimento legal do princípio da proporcionalidade, da retenção de dados e da transparência, uma vez que a aplicação da mesma garante o controlo do ciclo de vida dos dados e a rastreabilidade dos acessos, o que facilita auditorias da CNPD, enquanto autoridade de controlo, e do próprio Ministério Público.

A Diretiva (UE) 2022/2555 (NIS2) é igualmente uma opção de aplicação na metodologia interna dos sistemas de videovigilância, por prever a implementação de uma arquitetura técnica, procedimentos operacionais, existência de supervisão externa e integração legal. Considerando que a polícia é um organismo do Estado responsável pela segurança interna, a mesma é abrangida por esta diretiva em dois planos: no domínio de utilizador de sistemas críticos, pois implica auditorias de cibersegurança, planos de resposta a incidentes, redundância, encriptação de comunicações e monitorização contínua de redes; e como autoridade de notificação por falhas graves ou incidentes ao Centro Nacional de Cibersegurança. De igual forma, a Diretiva NIS2 institui formalmente a responsabilidade pela cibersegurança nos escalões superiores de gestão garantindo a sua integração nas estruturas de governação.

Desta análise verifica-se que a aplicação da Norma ISO/IEC 27001:2022 e da Diretiva NIS2, não só é possível à PSP e a todos os sistemas em uso pela PSP, como traria mais valias na gestão, operação, resiliência a ciberataques e processos administrativos dos sistemas informáticos envolvidos na videovigilância na via pública, garantindo a *accountability* dos seus utilizadores bem como o correto tratamento dos seus dados.

ESTUDO DA CONJUNTURA ATUAL

Análise aos pareceres da CNPD

Outro aspeto que não pode ser negligenciado no âmbito da verificação das medidas de segurança e do tratamento de dados pessoais são os diversos pareceres da CNPD. No decurso do pedido de autorização de instalação, está consagrado no n.º 3 do artigo 5.º da Lei n.º 95/2021 que a:

> decisão de autorização é precedida de parecer da Comissão Nacional de Proteção de Dados (CNPD), que se pronuncia sobre o pedido quanto ao cumprimento das regras referentes à segurança do tratamento dos dados recolhidos e do previsto nos n.os 4 a 6 do artigo 4.º e nos artigos 16.º, 18.º a 20.º e 22.º.

Esta análise da CNPD ao pedido de autorização de instalação e funcionamento de um sistema de videovigilância na via pública pretende, pois, pronunciar-se relativamente às proibições na instalação de câmaras em zonas destinadas a serem utilizadas em resguardo (n.º 4 do artigo 4.º da Lei n.º 95/2021), da recolha e tratamento dos dados pessoais e a possibilidade da utilização de um sistema de gestão analítica dos dados captados, por aplicação de critérios técnicos e proibição da captação e tratamento de dados biométricos (artigo 16.º da Lei n.º 95/2021), conservação e tratamento de imagens de factos com relevância criminal (artigo 18.º da Lei n.º 95/2021), direitos do titular dos dados nos termos dos artigos 13.º a 19.º da Lei n.º 59/2019 (artigo 20.º da Lei n.º 95/2021) e por fim, as condições de instalação (artigo 22.º da Lei n.º 95/2021). À CNPD compete ainda a fiscalização dos sistemas (artigo 24.º da Lei n.º 95/2021), mas face ao objetivo proposto com o presente estudo, não iremos dissertar sobre este aspeto.

No que concerne mais propriamente aos pareceres obrigatórios emitidos pela CNPD ao abrigo do já mencionado, e considerando o teor do estudo, analisaremos de seguida o seu conteúdo no que ao tratamento de dados diz respeito, com maior relevo para as medidas de segurança e medidas de mitigação de riscos identificadas nos diversos pareceres aos pedidos de instalação remetidos pela PSP. Considerando a relevância da Lei n.º 95/2021, apenas serão analisados os pareceres emitidos de 2022 a 2025, por terem sido emitidos na vigência da lei já mencionada.

Nos pedidos de autorização de instalação e funcionamento de sistemas de videovigilância, a CNPD tende a pronunciar-se com alguma regularidade sobre aspetos que que estão sob a alçada da responsabilidade do RTD, nomeadamente a rejeição de analítica de dados sem critérios fundamentados, face à ausência de definição e fundamentação dos critérios técnicos subjacentes, o que não permite a verificação do respeito pelos limites legais e a avaliação da proporcionalidade da sua utilização (CNPD, 2024b), tal como a restrição ao reconhecimento de matrículas, onde é recomendado que não seja utilizada essa tecnologia por não haver fundamento legal (CNPD, 2024f);

Existe ainda registo de considerações sobre as medidas de segurança da infraestrutura e comunicações, onde se incluem a segurança física e lógica de forma a garantir a integridade e confidencialidade dos dados (CNPD, 2024b). Neste campo, sugere ainda a CNPD (2024e) que deverá ser implementada proteção e alerta dos equipamentos em situações de tentativas de acesso não autorizado, adulteração e vandalismo (*anti-tampering*), bem como a existência de redundância e cópias de segurança (*backup*) (CNPD, 2024f). Aponta ainda a CNPD (2024e) que exista uma segregação de redes para mitigar riscos, bem como deve ser adotada uma política de gestão de senhas/credenciação nas câmaras ao invés das senhas de fábrica e reconfiguração da garantia da fidelidade da data e hora legal (CNPD, 2024f).

A CNPD (2022a, 2022b) refere também a necessidade de controlo de acessos de forma auditável para manter a rastreabilidade e limitação de privilégios de acesso aos dados, de acordo com o princípio do mínimo privilégio. São indicadas como medidas necessárias a implementação de autenticação reforçada com carácter individual e intransmissível, e se possível, com autenticação via RNSI (CNPD, 2024e). Outra medida mencionada é a criação de perfis de utilizador limitados, com acessos diferenciados, garantindo que operadores sem privilégios de administração não possam aceder a funções de manutenção ou modificação (CNPD, 2023b). No que respeita à extração de imagens e integridade dos dados, refere a CNPD (2022a, 2022b, 2022c, 2024f) que o sistema a instalar deve incluir mecanismos no *software* de gestão que permitam a exportação em formato digital, assinado digitalmente, para atestar a veracidade do conteúdo, bem como proteger a exportação com mecanismos de cifra ou senha. Nos registos de auditoria (*Logs*) é referida a necessidade de uma política de proteção/retenção dos registos de atividade e seus indicadores para os relatórios de auditoria (CNPD, 2024e), bem como deverão ser conservados os registos de auditoria (sem registo de dados pessoais) por um período de 2 (dois) anos, e armazenados em ambientes independentes do servidor de vídeo para proteger a sua integridade (CNPD, 2024e).

Por fim, e com especial relevância para o RTD, refere a CNPD (2022b, 2022c, 2023c) que a responsabilidade pelo tratamento dos dados cabe à força ou serviço de segurança requerente, independentemente da propriedade do equipamento. Embora a subcontratação sucessiva seja admissível, esta deve ser formalizada contratualmente (subcontratação e/ou sub-subcontratação) para a manutenção, substituição ou assistência do sistema, garantindo a auditabilidade das operações. Nesta formalização contratual deverá ficar expresso a delimitação do contrato ou acordo com o Município (subcontratante) e de eventuais sub-subcontratantes, por força do disposto no artigo 23.º da Lei n.º 59/2019 (CNPD, 2022b,

2023b, 2023c, 2024b). É ainda realçado que no contrato deve ser assegurado que não incorre uma inversão de papéis, mantendo a força requerente o domínio e controlo sobre o tratamento dos dados pessoais (CNPD, 2022b, 2022c, 2023c).

Verifica-se, pois, que a CNPD tende a pronunciar-se sobre responsabilidades do RTD, ou seja, sobre áreas que o RTD deverá ter especial preocupação na instrução dos processos de autorização, bem como na implementação e funcionamento concreto do sistema de videovigilância na via pública operado pela PSP.

Análise das entrevistas aos RTD

Uma vez enunciadas as funções e responsabilidades do RTD no contexto da utilização de sistemas de videovigilância na via pública pela PSP, bem como apresentadas as medidas de segurança da informação suscetíveis de aplicação para assegurar a salvaguarda, integridade e *accountability* dos dados pessoais, cumpre proceder a uma análise crítica no contexto prático da atuação diária da PSP.

Conforme já descrito anteriormente, para esta análise iremos apoiar-nos em entrevistas semi-estruturadas, aplicadas sob a forma de questionário online aos Chefes da Área Operacional dos comandos da PSP, ou de quem esteja a desempenhar as funções de RTD, com sistemas de videovigilância implementados. De acordo com as instruções da Direção Nacional da PSP, em concreto da Inspeção Nacional (através da Recomendação n.º 03/INSP/2024) e do Departamento de Operações (através de email difundido por todos os comandos), deverá ser nomeado como RTD para todos os sistemas desse comando o Chefe de Área Operacional .

No que concerne ao guião da entrevista realizada, o mesmo tem por base proceder a uma apreciação sistemática das competências, atividades, formação e desafios inerentes à função, sendo que foram analisadas 6 (seis) entrevistas validadas para o presente estudo, num universo total de 8 (oito) possíveis entrevistas (ao momento da elaboração deste estudo apenas 8 (oito) comandos possuem sistemas de videovigilância instalados e a funcionar).

Relativamente à análise das respostas recebidas, constata-se que a maioria dos entrevistados exerce as funções de Chefe de Área Operacional. Todavia, verificam-se situações em que o RTD corresponde, simultaneamente, ao 2º Comandante do respetivo comando (cf. entrevista n.º 4 e 6). Este facto evidencia a pluralidade de acumulação de funções, o que poderá suscitar implicações relevantes no exercício das funções de RTD.

Quanto ao tempo de desempenho das funções de RTD, verifica-se uma dispersão temporal, com períodos de experiência próximos de 2 (dois) anos (cf. entrevistas n.º 1 e 3), mas nos restantes constata-se um período temporal muito curto nas funções, que se afigura suscetível de gerar implicações significativas no conhecimento e exercício das respetivas funções, pela elevada rotatividade de funções dentro da PSP.

Quando questionados sobre o conhecimento das suas competências, foi possível aferir que o foco está na garantia da conformidade legal e na gestão operacional do sistema (cf. entrevistas n.º 1, 2, 3, 4, 5), mas em alguns casos com um conhecimento pouco profundo das suas competências e funções (cf. entrevista n.º 6). Estas responsabilidades incluem a verificação da conformidade legal e supervisão, mas simultaneamente incluem ainda uma vertente de controlo operacional e de auditoria dos sistemas.

Outro ponto relativamente ao qual se pretendeu proceder à recolha de informação consistiu na identificação do tipo de atividades desenvolvidas, tendo sido referido que estas se concentram na gestão diária, fiscalização e auditoria, tendo ainda o entrevistado n.º 4 referido que inclui nas suas atividades a identificação e implementação de medidas que permitam mitigar os riscos de uso indevido. Notou-se ainda uma preocupação (cf. entrevista n.º 2) na relação com as entidades externas (subcontratante e sub-subcontratantes) responsáveis pela prestação de apoio técnico, no cumprimento dos requisitos de acesso aos sistemas.

Pretendeu-se igualmente recolher resposta quanto a eventuais formações específicas para o desempenho das funções de RTD, tendo todos os inquiridos afirmado não ter recebido qualquer tipo de formação. Neste campo apura-se que o conhecimento resulta da experiência acumulada, da autoformação e da leitura da legislação e das normas internas de implementação.

No que se refere à existência de procedimentos internos de segurança, a maioria confirma a sua existência para definir mecanismos de segurança (cf. entrevistas n.º 2, 3, 4 e 5), maioritariamente consubstanciados em Normas de Execução Permanente (NEP) do comando. Verifica-se igualmente que as normas já em vigor nos comandos não foram alteradas pelos entrevistados (cf. entrevistas n.º 3 e 4).

Outro ponto que se pretendeu avaliar foi a (in)segurança dos dados durante o tratamento, tendo sido unânime a resposta que sentem que o sistema é seguro, com pouca probabilidade de existência de violações ou incidentes críticos.

Relativamente ao acompanhamento do funcionamento dos sistemas é referido que este inclui o acompanhamento presencial e da troca de correspondência por email (cf. entrevista n.º 2), feedback regular de quem opera o sistema (cf. entrevista n.º 5). Apesar de alguns entrevistados manifestarem a intenção de acompanhar com maior regularidade, não o fazem e apontam como justificação o volume, multiplicidade e complexidade de outras tarefas, manifestando que a falta de regularidade não é a mais adequada à sensibilidade da matéria (cf. entrevista n.º 3).

Por último, quando questionados que medidas poderiam ser implementadas para melhorar os conhecimentos e desempenho das funções de RTD, apurou-se que todos os entrevistados indicam como medida primordial a implementar a formação especifica na área (cf. entrevistas n.º 1, 2, 3, 4, 5, 6). Outras sugestões passam pela partilha de conhecimento entre os vários responsáveis, vertida em documento nacional nesta temática (cf. entrevista n.º 3), concentração de recursos com o conhecimento técnico para um acompanhamento mais próximo (cf. entrevista n.º 4) e a necessidade de resolver questões técnicas com maior celeridade (cf. entrevista n.º 2).

Assim, analisadas as respostas fornecidas pelos entrevistados, é possível aferir, em termos gerais, que o conhecimento das funções e responsabilidades de RTD, está diretamente relacionado com o tempo de exercício dessas funções, refletindo maior experiência e compreensão das medidas técnicas e organizativas sob sua responsabilidade quanto maior for o tempo de exercício das funções. Constata-se, contudo, que as atividades desenvolvidas se concentram, em geral, em tarefas de natureza operacional, sem a devida prioridade à elaboração de procedimentos internos que assegurem o correto tratamento dos dados e aumente a resiliência dos sistemas. Adicionalmente, ressalta-se, de forma quase unânime, a existência/constatação de uma lacuna quanto à formação específica em matéria de RGPD e das medidas técnicas e organizativas necessárias.

CONCLUSÃO

Concluído o estudo, a sistematização dos resultados das análises e o enquadramento jurídico-formal com a realidade prática, poderemos responder cabalmente às hipóteses e objetivos propostos.

Da análise efetuada no presente estudo, podemos aferir que relativamente à primeira hipótese (saberão os RTD nomeados as suas funções e responsabilidades) constata-se que,

através das entrevistas, a maioria dos RTD foca a sua atividade na garantia da conformidade legal e na gestão operacional dos sistemas, mas sem um conhecimento profundo sobre as suas competências e atribuições. O conhecimento tende a estar diretamente relacionado com o tempo de experiência.

Quanto à segunda hipótese (os RTD têm à sua disposição as ferramentas necessárias para o bom desempenho das suas funções e responsabilidades), verifica-se que neste momento existem procedimentos internos (maioritariamente NEP dos comandos), sendo que a nível interno foi identificada uma lacuna crítica: a ausência de formação específica nesta área (RGPD e medidas técnicas e organizativas). O conhecimento é, assim, fruto do autoconhecimento e experiência acumulada.

Por último, quanto à terceira hipótese (que necessidades sentem os RTD quando estão no desempenho das funções) a principal necessidade passa por criar uma formação específica e especializada na área da proteção de dados e videovigilância em consonância com o quadro legal português. Pode também ser apontada como necessidade a criação de um documento de carácter nacional, onde esteja vertida esta informação e que esteja disponível a quem dela necessite.

No que concerne ao primeiro objetivo de investigação (Analisar e sistematizar o enquadramento legal aplicável à videovigilância na via pública e ao RTD em sistemas de videovigilância da PSP), verifica-se que o regime jurídico em Portugal é complexo e multinível, com aplicação primordial da Lei n.º 95/2021 e da Lei n.º 59/2019, numa perspetiva de garantia da conformidade legal, supervisão independente e responsabilidades acrescidas no tratamento de dados pessoais.

Relativamente ao segundo objetivo (Definir as funções, responsabilidades e perfil de competências do RTD na PSP), o estudo confirmou o papel fulcral do RTD na garantia da conformidade legal, técnica e organizacional do tratamento de dados. O RTD é a entidade competente que determina as finalidades e os meios de tratamento, com responsabilidades cruciais na elaboração da AIPD, de adoção de medidas técnicas e organizativas apropriadas para garantir a segurança, integridade e confidencialidade dos dados, a manutenção de registos de auditoria, a notificação de violações de dados, bem como a regulação formal da subcontratação.

Finalmente no que respeita ao terceiro objetivo (Desenvolver recomendações/melhorias para a criação de um protocolo interno de atuação e *accountability* nas funções do RTD), o estudo aponta para a necessidade premente de se elaborar um

documento de normalização nacional para suprir a lacuna formativa e instituir um protocolo interno robusto, onde sejam listadas as boas práticas de segurança identificadas, as metodologias e as normas em vigor, propondo a criação de um procedimento de normalização, através da adoção de uma norma de execução permanente de âmbito nacional (vide Apêndice A). A adoção de normas já reconhecidas, tal como a ISO/IEC 27001:2022 e a Diretiva NIS2, surgem como uma mais-valia.

Em suma, apesar dos vinte anos da legislação que regula a videovigilância, o conhecimento das funções e competências do RTD no seio da PSP ainda tem um longo caminho quanto à consciencialização das suas funções, competências e atribuições.

BIBLIOGRAFIA

Canotilho, G. e Moreira, V. (2008) Constituição da República Portuguesa Anotada, v I, Coimbra Editora

Centro Nacional de Cibersegurança – CNCS, 2019. *Quadro Nacional de Referência para a Cibersegurança (QNRCS)* (V. 2.0), https://www.cncs.gov.pt/docs/cncs-qnrcs-2019.pdf

Comissão Nacional de Proteção de Dados – CNPD. (2022a). Parecer/2022/18, de 2 de março de 2022, disponível em https://www.cnpd.pt/decisoes/historico-de-decisoes/?year=2022&type=4&ent=Secretaria+de+Estado+da+Administração+Interna&pgd=2

Comissão Nacional de Proteção de Dados – CNPD. (2022b). Parecer/2022/102, de 15 de novembro de 2022, disponível em https://www.cnpd.pt/decisoes/historico-de-decisoes/?year=2022&type=4&ent=Secretaria+de+Estado+da+Administração+Interna&pgd=1

Comissão Nacional de Proteção de Dados – CNPD. (2022c). Parecer/2022/107, de 18 de novembro de 2022, disponível em https://www.cnpd.pt/decisoes/historico-de-decisoes/?year=2022&type=4&ent=Secretaria+de+Estado+da+Administração+Interna&pgd=1

Comissão Nacional de Proteção de Dados – CNPD. (2023a), Diretriz/2023/1, de 10 de janeiro de 2023;

Comissão Nacional de Proteção de Dados – CNPD. (2023b). Parecer/2023/58, de 16 de junho de 2023, disponível em https://www.cnpd.pt/decisoes/historico-de-decisoes/?year=2023&type=4&ent=Secretaria+de+Estado+da+Administração+Interna

Comissão Nacional de Proteção de Dados – CNPD. (2023c). Parecer/2023/74, de 25 de julho de 2023, disponível em https://www.cnpd.pt/decisoes/historico-de-decisoes/?year=2023&type=4&ent=Secretaria+de+Estado+da+Administração+Interna

Comissão Nacional de Proteção de Dados – CNPD. (2024a). Parecer/2024/17, de 6 de junho de 2024, disponível em https://www.cnpd.pt/decisoes/historico-de-decisoes/?year=2024&type=4&ent=

Comissão Nacional de Proteção de Dados – CNPD. (2024b). Parecer/2024/18, de 11 de junho de 2024, disponível em https://www.cnpd.pt/decisoes/historico-de-decisoes/?year=2024&type=4&ent=

Comissão Nacional de Proteção de Dados – CNPD. (2024c). Parecer/2024/19, de 26 de junho de 2024, disponível em https://www.cnpd.pt/decisoes/historico-de-decisoes/?year=2024&type=4&ent=

Comissão Nacional de Proteção de Dados – CNPD. (2024d). Parecer/2024/38, de 27 de agosto de 2024, disponível em https://www.cnpd.pt/decisoes/historico-de-decisoes/?year=2024&type=4&ent=

Comissão Nacional de Proteção de Dados – CNPD. (2024e). Parecer/2024/40, de 15 de outubro de 2024, disponível em https://www.cnpd.pt/decisoes/historico-de-decisoes/?year=2024&type=4&ent=

Comissão Nacional de Proteção de Dados – CNPD. (2024f). Parecer/2024/54, de 3 de dezembro de 2024, disponível em https://www.cnpd.pt/decisoes/historico-de-decisoes/?year=2024&type=4&ent=

Diretiva (EU) 2016/680, do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho, https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016L0680 ;

Diretiva (UE) 2022/2555 – NIS2, do Parlamento Europeu e do Conselho de 14 de dezembro de 2022 relativa a medidas destinadas a garantir um elevado nível comum e cibersegurança na União que altera o Regulamento (UE) n.o 910/2014 e a Diretiva UE) 2018/1972 e revoga a Diretiva (UE) 2016/1148 (Diretiva SRI 2), https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32022L2555

European Data Protection Board, Diretriz 3/2019 sobre tratamento de dados pessoais através de dispositivos de vídeo, versão 2 (2020), https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_pt.pdf

Foucault, M., (1987), *Vigiar e punir*, 20º ed., Editora Vozes.

Frias, J. (2024), *A utilização de sistemas de videovigilância pela Polícia de Segurança Pública: A senda para a instrução de um pedido de autorização*, Trabalho Individual

Final do Curso de Direção e Estratégia Policial. ISCPSI. http://hdl.handle.net/10400.26/54356

Frois, C., (2011), *Vigilância e Poder*. Editora Mundos Sociais.

Gabinete Nacional de Segurança – GNS (2018), RGPD e a segurança das redes e sistemas de informação – Manual de boas práticas, parte III – Segurança Física, https://www.gns.gov.pt/docs/boas-praticas-iii.pdf

Inácio, A. (2018). *A sociedade de risco, as T.I. e o exercício da liberdade em segurança. Tratamento de dados pessoais pelas forças e serviços de segurança*. In T. Rodrigues & M. Painho (Eds.), *Modelos Preditivos e Segurança Pública*. (pp. 45-56). Fronteira do Caos Editores Lda

Lei n.º 2/2004, de 12 de maio, Estabelece o regime temporário da organização da ordem pública e da justiça no contexto extraordinário da fase final do Campeonato Europeu de Futebol - Euro 2004, Diário da República n.º 111/2004, Série I-A, https://diariodarepublica.pt/dr/detalhe/lei-organica/2-2004-264283

Lei n.º 1/2005, de 10 de janeiro, Regula a utilização de câmaras de vídeo pelas forças e serviços de segurança em locais públicos de utilização comum, Diário da República n.º 6/2005, Série I-A, https://diariodarepublica.pt/dr/detalhe/lei/1-2005-457049

Lei n.º 53/2007, de 31 de agosto (na sua última versão com as alterações introduzidas pela Lei n.º 55-C/2025) – aprova a orgânica da Polícia de Segurança Pública. https://dre.pt/dre/legislacao-consolidada/lei/2007-174279072

Lei n.º 9/2012, de 23 de fevereiro, Procede à terceira alteração à Lei n.º 1/2005, de 10 de janeiro, que regula a utilização de câmaras de vídeo pelas forças e serviços de segurança em locais públicos de utilização comum, Diário da República n.º 39/2012, Série I, https://diariodarepublica.pt/dr/detalhe/lei/9-2012-542867

Lei n.º 58/2019, de 8 de agosto, assegura a execução, na ordem jurídica nacional, do Regulamento (UE) 2016/679 do Parlamento e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Diário da República 1.ª Série. n.º 151, disponível em https://diariodarepublica.pt/dr/detalhe/lei/58-2019-123815982

Lei n.º 59/2019, de 8 de agosto, 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. Diário da República 1.ª Série. n.º 151, disponível em https://diariodarepublica.pt/dr/detalhe/lei/59-2019-123815983

Lei n.º 95/2021, de 29 de dezembro, regula a utilização e o 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, revogando a Lei n.º 1/2005, de 10 de janeiro. Diário da República 1.ª Série. n.º 251, disponível em https://diariodarepublica.pt/dr/detalhe/lei/95-2021-176714548

Melo, P. & Viseu, A. (2024), *20 anos de videovigilância dos espaços públicos em Portugal: panorama e desafios sociopolíticos*. Comunicação Pública, 19 (37). https://doi.org/10.34629/cpublica.855

Morais, J. (2024), *Tratamento de dados pessoais: sugestões para melhoria dos procedimentos na Polícia de Segurança Pública em concursos e publicações internas*, Trabalho Individual Final do Curso de Comando e Direção Policial, ISCPSI, http://hdl.handle.net/10400.26/46024

Moreira, L., 2017, *Videovigilância no espaço público em Portugal: em busca de um rumo*, Trabalho Individual Final do Curso de Direção e Estratégia Policial. ISCPSI. http://hdl.handle.net/10400.26/35248

Organização Internacional de Normalização (ISO). (2022). ISO 27001:2022 - Information security, cybersecurity, and privacy protection — Information security management systems

Pereira, D. (2019), *O sistema de videovigilância – prevenção e investigação criminais*, Dissertação de mestrado, Universidade Nova de Lisboa, http://hdl.handle.net/10362/66763;

Pereira, L. (2017), *Políticas de Segurança e a videovigilância urbana – o caso da Amadora*, Trabalho Individual Final do Curso de Direção e Estratégia Policial. ISCPSI http://hdl.handle.net/10400.26/35180

Piza E., Welsh B., Farrington D., Thomas A. (2019), *CCTV Surveillance for crime prevention: A 40-year systematic review with meta-analysis*. Criminology & Public Policy. 2019;18. Pp.135–159. https://doi.org/10.1111/1745-9133.12419

Polícia de Segurança Pública – PSP (2024), Recomendação n.º 03/INSP/2024 – Recomendação relativa à instalação e gestão de sistemas de videovigilância no espaço público.

Portaria n.º 372/2012, de 16 de novembro, fixa os requisitos técnicos mínimos das câmaras fixas e portáteis de videovigilância, https://diariodarepublica.pt/dr/detalhe/portaria/372-2012-191103

Procuradoria-Geral da República, Parecer n.º 10/2017 de 28 de julho de 2017, Diário da República 2.ª série — N.º 145

Regulamento (UE) 2016/679, do Parlamento Europeu e do Conselho, de 27 de abril de 2016 - RGPD, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva n.º 95/46/CE sobre a Proteção de Dados. Jornal Oficial da União Europeia (04.05.2016) Série L. n.º 119, disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679

Regulamento (UE) 2024/2847 do Parlamento Europeu e do Conselho de 23 de outubro de 2024 - Regulamento de Ciber-Resiliência, relativo aos requisitos horizontais de cibersegurança dos produtos com elementos digitais e que altera os Regulamentos (UE) n.º 168/2013 e (UE) 2019/1020 e a Diretiva (UE) 2020/1828, https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=OJ:L_202402847

Resolução do Conselho de Ministros n.º 50/88, de 3 de dezembro – SEGNAC 1, que aprova as Instruções para a Segurança Nacional, Salvaguarda e Defesa das Matérias Classificadas, Diário da República 1ª série

Resolução do Conselho de Ministros n.º 37/89, de 24 de outubro - SEGNAC 2, que aprova as Normas para a Segurança Nacional, Salvaguarda e Defesa das Matérias Classificadas, Segurança Industrial, Tecnológica e de Investigação, Diário da República 1ª série

Resolução do Conselho de Ministros n.º 16/94, de 22 de março – SEGNAC 3, que aprova as Instruções para a Segurança Nacional, Segurança das Telecomunicações, Diário da República 1ª-B série

Rodrigues, M. (2024), *A Videovigilância no espaço público: dificuldades e dilemas no processo de implementação*, Trabalho Individual Final do Curso de Direção e Estratégia Policial. ISCPSI. http://hdl.handle.net/10400.26/54357

Silva**,** A. (2024). *20 anos de videovigilância dos espaços públicos em Portugal: panorama e desafios sociopolíticos***.** Cpública

Silva, L. (2024) , *A proteção de dados pessoais – auditoria e controlo interno no âmbito das competências da Inspeção Nacional da Polícia de Segurança Pública*, Trabalho

Individual Final do Curso de Direção e Estratégia Policial. ISCPSI. http://hdl.handle.net/10400.26/54355

APÊNDICE A

Proposta de estrutura de norma: "Responsável pelo Tratamento dados – videovigilância na via pública" (de acordo com a organização, elaboração e distribuição de normas de execução permanente – NEP ASDDN/GEP/00/00)

Enquadramento Legal

1. **Finalidade**
   a. Definir e clarificar o quadro legal, as funções, as responsabilidades e competências do Responsável pelo Tratamento de Dados (RTD), no domínio da segurança, proteção e tratamento dos dados pessoais decorrentes do uso de sistemas de videovigilância na via pública;

2. **Âmbito**
   a. Aplica-se a todos os profissionais que desempenham as funções de RTD na Polícia de Segurança Pública

3. **Procedimentos**

   a. **Nomeação do RTD** – para o exercício das funções de RTD, é nomeado o Chefe de Área Operacional do Comando territorialmente competente onde se pretende instalar o sistema de videovigilância na via pública;

   b. Funções e responsabilidades do RTD
      i. Garantia da conformidade legal, técnica e organizacional do tratamento dos dados
         1. Medidas técnicas e organizativas
            a. Medidas de segurança física
            b. Medidas de segurança eletrónica
         2. Auditorias
         3. Avaliação de risco
         4. Avaliação de Impacto sobre a Proteção de Dados

5. Colaboração com a autoridade de controlo – CNPD

c. Medidas organizativas e técnicas para a segurança da informação

i. (descrição das medidas passíveis de implementação)

d. Gestão de incidentes e violações de dados

i. Política de gestão de incidentes
ii. Definição de violação
iii. Notificação à CNPD
iv. Comunicação aos titulares dos dados
v. Documentação de auditorias

e. Relação com os subcontratantes

i. Contrato de subcontratação e sub-subcontratação

f. Relação com o Encarregado de Proteção de Dados

4. Disposições finais

ANEXOS

ANEXO N.º 1 - ENTREVISTA N.º 1

1. **Funções desempenhadas?**

Chefe de Área Operacional

2. **Desde quando desempenha as funções de responsável pelo tratamento de dados do sistema de videovigilância na via pública?**

Há quase dois anos.

3. **Enquanto responsável pelo tratamento de dados pessoais, quais são as suas competências e atribuições?**

As decorrentes da Lei de proteção de dados, no que se refere ao controlo e supervisão do sistema e respetivo uso das informações.

4. **No âmbito da sua atividade de responsável pelo tratamento de dados, que tipo de atividades desenvolve (ex.: atividades de rotina, autorizações, auditorias, elaboração de procedimentos...)**

Garantir o registo e auditabilidade de todas as ações desenvolvidas pelos operadores; estabelecer, nos novos sistemas o cumprimento dos requisitos de aceso por parte das empresas subcontratadas; verificar o cumprimento das normas no que à gravação e extração de dados diz respeito.

5. **Desde o início do funcionamento do sistema de videovigilância na via pública teve algum tipo de formação específica para o desempenho das funções já descritas? Se sim, quais e ministradas por quem?**

Não tive qualquer tipo de formação.

6. **Existem procedimentos internos estabelecidos para definir mecanismos de segurança? Se sim, quais e quem os definiu?**

Especificamente relacionado com o CCTV, não. É garantido o registo de todos os acessos e com que finalidade.

7. **Durante a operação do(s) sistema(s) de videovigilância na via pública sentiu que a segurança dos dados poderia estar em causa de alguma forma?**

Não.

8. **Enquanto responsável pelo tratamento de dados pessoais, como acompanha o funcionamento, operação e manutenção do sistema?**

Através da realização de visitas e confirmação do cumprimento das regras de acesso.

9. **Da sua experiência, que medidas poderiam ser implementadas para melhorar os seus conhecimentos e desempenho enquanto responsável pelo tratamento de dados pessoais?**

Formação específica na área, tanto na vertente da utilização como na vertente da conceção, organização e implementação das diversas fases do processo de autorização

ANEXO N.º 2 - ENTREVISTA N.º 2

1. **Funções desempenhadas?**

Chefe da Área Operacional do CD Coimbra desde abril de 2024. Antes Comandante de Divisão Policial de Coimbra em acumulação, janeiro a abril de 2024. Chefe da Área de Apoio do CD Coimbra de outubro de 2020 a abril de 2024.

2. **Desde quando desempenha as funções de responsável pelo tratamento de dados do sistema de videovigilância na via pública?**

Desde abril de 2024.

3. **Enquanto responsável pelo tratamento de dados pessoais, quais são as suas competências e atribuições?**

Organização dos processos de renovação das autorizações e/ou novos processos. Autorização de visualização e gravação de imagens. Elaboração de procedimentos relativos a pedidos de gravação de imagens, visualização e circuito das imagens gravadas. Chefia direta dos elementos que visualizam as imagens em tempo real.

4. **No âmbito da sua atividade de responsável pelo tratamento de dados, que tipo de atividades desenvolve (ex.: atividades de rotina, autorizações, auditorias, elaboração de procedimentos...)**

Autorizações de visualização/gravação, elaboração de procedimentos, verificação dos contatos com as pessoas/empresas/municípios responsáveis para prestação de apoio técnico.

5. **Desde o início do funcionamento do sistema de videovigilância na via pública teve algum tipo de formação específica para o desempenho das funções já descritas? Se sim, quais e ministradas por quem?**

Fui responsável pelo início do processo de videovigilância em Coimbra, em 2007/08/09, na altura no Núcleo de Operações. Nem no início, nem nos anos que se seguiram tive qualquer formação nesta matéria.

6. **Existem procedimentos internos estabelecidos para definir mecanismos de segurança? Se sim, quais e quem os definiu?**

Sim. O Comando tem uma NEP sobre esta matéria.

7. **Durante a operação do(s) sistema(s) de videovigilância na via pública sentiu que a segurança dos dados poderia estar em causa de alguma forma?**

Não, nunca.

8. **Enquanto responsável pelo tratamento de dados pessoais, como acompanha o funcionamento, operação e manutenção do sistema?**

Presencialmente, considerando que a visualização em tempo real e após, é feita junto do CCC, na sede do Comando e acompanhando a troca de correspondência por email, entre os operadores envolvidos e os serviços

9. **Da sua experiência, que medidas poderiam ser implementadas para melhorar os seus conhecimentos e desempenho enquanto responsável pelo tratamento de dados pessoais?**

Neste momento as limitações sentidas prendem-se mais com a parte prática e operacional do funcionamento do sistema. A falta de capacidade em resolver rapidamente questões técnicas, pela dependência de outros, externos á instituição e também com a falta de efetivo para

acompanhar todas as câmaras, considerando que continuamos a alargar a área sob videovigilância.

Nesta fase, o conhecimento já chegou pelos anos de experiência, apesar de ser sempre benéfico formação, tanto para a signatária como para os elementos que todos os dias estão em frente aos monitores. Com o aumento do n.º de câmaras surge o aumento de pedidos de visualização de imagens, para posterior gravação e utilização como meio de prova, que colocam outras dificuldades em termos de efetivo e de material para gravação.

ANEXO N.º 3 - ENTREVISTA N.º 3

1. **Funções desempenhadas?**

2º Comandante Distrital e Chefe da Área Operacional, em acumulação.

2. **Desde quando desempenha as funções de responsável pelo tratamento de dados do sistema de videovigilância na via pública?**

2 Anos.

3. **Enquanto responsável pelo tratamento de dados pessoais, quais são as suas competências e atribuições?**

Adotar todas as medidas técnicas e organizativas que salvaguardem os princípios legalmente aplicáveis ao tratamento de dados pessoais, garantindo permanentemente a sua conformidade legal, bem como encontrar-se permanentemente preparado para demonstrar que o tratamento dos dados respeita integralmente a Lei. Paralelamente deve regularmente avaliar se as medidas adotadas se mostram adequadas aos seus objetivos, procedendo à sua alteração/atualização sempre que se mostre adequado, conforme decorre das responsabilidades que se lhe encontram legalmente acometidas, pela Lei 59/2019.

4. **No âmbito da sua atividade de responsável pelo tratamento de dados, que tipo de atividades desenvolve (ex.: atividades de rotina, autorizações, auditorias, elaboração de procedimentos...)**

Auditorias regulares à utilização do sistema. Auditorias especificas relativamente aos procedimentos de extração de imagens, verificando a sua conformidade legal.

Verificação do cumprimento dos normativos internos estabelecidos. Verificação periódica dos utilizadores e perfis de acesso.

5. **Desde o início do funcionamento do sistema de videovigilância na via pública teve algum tipo de formação específica para o desempenho das funções já descritas? Se sim, quais e ministradas por quem?**

Nunca tive formação específica nesta área e para esta função. O pouco conhecimento que disponho resulta do estudo dos preceitos legais e troca de informações com outros polícias com as mesmas atribuições.

6. **Existem procedimentos internos estabelecidos para definir mecanismos de segurança? Se sim, quais e quem os definiu?**

Existem. Foram estabelecidos e implementados pelo meu antecessor no cargo, quando iniciou o funcionamento do primeiro sistema no comando.
Ainda se mostram atuais e adequados aos fins pretendidos.

7. **Durante a operação do(s) sistema(s) de videovigilância na via pública sentiu que a segurança dos dados poderia estar em causa de alguma forma?**

Não, de todo. Não obstante, tenho sempre presente que esse risco existe, pelo que são adotadas medidas para o minimizar, mas como declaramos internamente, não existem situações de risco zero.

8. **Enquanto responsável pelo tratamento de dados pessoais, como acompanha o funcionamento, operação e manutenção do sistema?**

Acompanho o funcionamento e operação do sistema, com a maior regularidade que me é possível, devendo reconhecer que dada a multiplicidade de responsabilidades e tarefas, não será a regularidade mais adequada, considerando a sensibilidade desta matéria.

9. **Da sua experiência, que medidas poderiam ser implementadas para melhorar os seus conhecimentos e desempenho enquanto responsável pelo tratamento de dados pessoais?**

Uma das questões fundamentais parece-me ser dotado de formação específica nesta área.

Outra solução seria a partilha entre os vários responsáveis pelo tratamento de dados, convertida num documento nacional que elencasse várias possibilidades, que pudesse constituir-se como uma espécie de "Guião". Estou convicto (excluindo o signatário) que já existe um manancial expressivo de experiência acumulada da PSP nesta e outras áreas, mas encontra-se dispersa e centrada em policias individualmente considerados, o que, quando mudam de função, acaba por provocar o seu desvanecimento ou perda.

ANEXO N.º 4 - ENTREVISTA N.º 4

1. **Funções desempenhadas?**

Chefe da Área Operacional.

2. **Desde quando desempenha as funções de responsável pelo tratamento de dados do sistema de videovigilância na via pública?**

Desde janeiro de 2025.

3. **Enquanto responsável pelo tratamento de dados pessoais, quais são as suas competências e atribuições?**

Genericamente a sua competência é garantir que o uso de imagens e informações produzidas pelo sistema de vigilância esteja em conformidade com a legislação existente nesta matéria, ao mesmo tempo que garante ainda a sua transparência e limitação do seu uso à sua finalidade.

4. **No âmbito da sua atividade de responsável pelo tratamento de dados, que tipo de atividades desenvolve (ex.: atividades de rotina, autorizações, auditorias, elaboração de procedimentos...)**

As funções são variadas desde as relacionadas com a atividade diária produzida pelo sistema, como seja a avaliação de pedido, a autorização da preservação de imagens e a sua extração, a garantia dos acessos restritos, até outras de maior abrangência do sistema como um todo nas quais se inclui as auditorias e a identificação e implementação de medidas que permitam mitigar os riscos de uso indevido.

5. **Desde o início do funcionamento do sistema de videovigilância na via pública teve algum tipo de formação específica para o desempenho das funções já descritas? Se sim, quais e ministradas por quem?**

Não. Apenas autoformação através da leitura da legislação e normas internas de implementação.

6. **Existem procedimentos internos estabelecidos para definir mecanismos de segurança? Se sim, quais e quem os definiu?**

Existe uma Norma de Execução Permanente (NEP) que enquadra os normativos internos relativos ao funcionamento do Centro de Comando e Controlo de Videovigilância (CCCV), criado na sequência da autorização para a implementação de um sistema de videovigilância na cidade do Porto e que estabelece vários mecanismos de segurança para todos os envolvidos.

7. **Durante a operação do(s) sistema(s) de videovigilância na via pública sentiu que a segurança dos dados poderia estar em causa de alguma forma?**

Embora seja uma experiência ainda de curta duração nunca senti que a segurança dos dados pudesse não estar em segurança.

8. **Enquanto responsável pelo tratamento de dados pessoais, como acompanha o funcionamento, operação e manutenção do sistema?**

Acompanho com especial interesse e preocupação dada a sensibilidade da matéria. contudo, dados os afazeres de um Chefe de Área Operacional de um Comando Metropolitano, caraterizados pelo volume, complexidade e heterogeneidade dos assuntos com que lida, o acompanhamento acaba por não ser direto e específico.

9. **Da sua experiência, que medidas poderiam ser implementadas para melhorar os seus conhecimentos e desempenho enquanto responsável pelo tratamento de dados pessoais?**

Realização de maior formação específica na matéria. Atenta a importância e sensibilidade da matéria em análise deveria esta matéria estar concentrada numa figura que assegurasse um melhor/mais próximo acompanhamento. Deveria ser criado um documento que definisse especificamente as diretrizes e responsabilidades do responsável pelo tratamento de dados.

ANEXO N.º 5 - ENTREVISTA N.º 5

1. **Funções desempenhadas?**

Chefe da Área Operacional

2. **Desde quando desempenha as funções de responsável pelo tratamento de dados do sistema de videovigilância na via pública?**

31 de julho de 2025.

3. **Enquanto responsável pelo tratamento de dados pessoais, quais são as suas competências e atribuições?**

Assegurar que o sistema está a operar de acordo com a respetiva autorização. Promover auditorias ao seu funcionamento (inclui procedimentos). Garantir que as medidas técnicas e organizativas estão em vigor.

4. **No âmbito da sua atividade de responsável pelo tratamento de dados, que tipo de atividades desenvolve (ex.: atividades de rotina, autorizações, auditorias, elaboração de procedimentos...)**

Verificação de rotina do funcionamento do sistema. Impulsionar e supervisionar os regulamentos necessários. Promover auditorias. Ligação com a entidade externa dona do sistema (CMPDL).

5. **Desde o início do funcionamento do sistema de videovigilância na via pública teve algum tipo de formação específica para o desempenho das funções já descritas? Se sim, quais e ministradas por quem?**

Não.

6. **Existem procedimentos internos estabelecidos para definir mecanismos de segurança? Se sim, quais e quem os definiu?**

Sim. NEP do CRA. Definida pelo CRA, tendo por base modelos de outros Comandos.

7. **Durante a operação do(s) sistema(s) de videovigilância na via pública sentiu que a segurança dos dados poderia estar em causa de alguma forma?**

Não. O acesso ao sistema é restrito e condicionado.

8. **Enquanto responsável pelo tratamento de dados pessoais, como acompanha o funcionamento, operação e manutenção do sistema?**

Feedback regular do funcionamento do sistema, o que inclui avarias e necessidades de intervenção, assim como informação regular sobre os pedidos de imagens, para efeitos de carrear elementos de prova para investigações (em sede de inquérito - com NUIPC).

9. **Da sua experiência, que medidas poderiam ser implementadas para melhorar os seus conhecimentos e desempenho enquanto responsável pelo tratamento de dados pessoais?**

Formação na área RGPD.

ANEXO N.º 6 - ENTREVISTA N.º 6

1. **Funções desempenhadas?**

2º Comandante.

2. **Desde quando desempenha as funções de responsável pelo tratamento de dados do sistema de videovigilância na via pública?**

Desde maio de 2025.

3. **Enquanto responsável pelo tratamento de dados pessoais, quais são as suas competências e atribuições?**

Para ser totalmente honesto, desconheço.

4. **No âmbito da sua atividade de responsável pelo tratamento de dados, que tipo de atividades desenvolve (ex.: atividades de rotina, autorizações, auditorias, elaboração de procedimentos...)**

Até ao momento não foram realizadas quaisquer atividades.

5. **Desde o início do funcionamento do sistema de videovigilância na via pública teve algum tipo de formação específica para o desempenho das funções já descritas? Se sim, quais e ministradas por quem?**

Até a presente data ainda não recebi formação específica quanto ao sistema instalado na cidade.

6. **Existem procedimentos internos estabelecidos para definir mecanismos de segurança? Se sim, quais e quem os definiu?**

Desconheço.

7. **Durante a operação do(s) sistema(s) de videovigilância na via pública sentiu que a segurança dos dados poderia estar em causa de alguma forma?**

Não me considero qualificado o suficiente para poder responder a essa questão.

8. **Enquanto responsável pelo tratamento de dados pessoais, como acompanha o funcionamento, operação e manutenção do sistema?**

Não acompanho.

9. **Da sua experiência, que medidas poderiam ser implementadas para melhorar os seus conhecimentos e desempenho enquanto responsável pelo tratamento de dados pessoais?**

Receber formação específica sobre o tratamento de dados.