Câmeras no trabalho: dez regras para evitar riscos à privacidade e cumprir a LGPD

Especialistas orientam empresas sobre finalidade do monitoramento, acesso às gravações, segurança e prazo de armazenamento

As câmeras de segurança são utilizadas por empresas para proteger o patrimônio, monitorar acessos e apoiar a prevenção e a apuração de incidentes. Quando registram pessoas identificadas ou identificáveis, seu uso envolve tratamento de dados pessoais e exige cuidados com a proteção desses dados e com a privacidade das pessoas filmadas.

A Axis AI & Privacy Governance reúne dez pontos para orientar empresas na gestão do videomonitoramento, da escolha dos locais de instalação ao controle de acesso e à eliminação das imagens. O objetivo é ajudar as organizações a definir regras claras, reduzir riscos e acompanhar o uso dos equipamentos ao longo do tempo.



cristianstorto_CANVA

1. Definir a finalidade do monitoramento

A empresa deve identificar qual problema pretende enfrentar e documentar a finalidade da captação. Proteger pessoas e controlar acessos são objetivos que precisam ser delimitados. Câmeras instaladas para segurança não devem ser usadas rotineiramente para medir produtividade ou fiscalizar pausas de seus empregados e demais colaboradores.

2. Avaliar os locais e o enquadramento

Entradas, corredores, recepções e estacionamentos podem ser monitorados quando houver um motivo justo para isso. Banheiros, vestiários e espaços de troca de roupa devem ficar fora do monitoramento. Em clínicas médicas, é preciso preservar a privacidade de consultas, exames e procedimentos.

3. Informar sobre o uso das câmeras

As áreas monitoradas devem ser sinalizadas. Além disso, as pessoas também precisam ter acesso a informações sobre quem é responsável pelo tratamento das imagens captadas, para quais finalidades as imagens são captadas, por quanto tempo as imagens são armazenadas e como podem exercer seus direitos.

4. Definir quem pode acessar as imagens

As permissões devem corresponder às necessidades de cada função. Visualizar imagens ao vivo e exportar arquivos são atividades distintas, por isso consultas e exportações devem ser justificadas e registradas, com revisão periódica dos acessos. O sistema deve utilizar contas individuais, senhas fortes e autenticação multifator, especialmente no acesso remoto. Senhas de fábrica precisam ser substituídas, e os acessos devem ser revogados quando uma pessoa deixa a empresa ou muda de função. Contas compartilhadas dificultam identificar quem consultou ou extraiu uma imagem.

5. Proteger senhas e contas

Câmeras e aplicativos precisam de atualizações e configurações seguras: o acesso remoto deve utilizar conexões protegidas, com medidas como segmentação da rede e criptografia, conforme os riscos envolvidos. A empresa também deve acompanhar a segurança dos sistemas utilizados, verificando se as configurações e os mecanismos de proteção permanecem adequados ao longo do tempo.

6. Manter equipamentos e fornecedores sob controle

Contratos com instaladores, empresas de vigilância e provedores de armazenamento em nuvem devem estabelecer claramente as responsabilidades de cada parte no tratamento das imagens. É importante definir limites de acesso, requisitos de segurança da informação, condições de armazenamento, procedimentos para compartilhamento e eliminação dos registros, além de protocolos para comunicação e resposta a incidentes. A empresa contratante deve acompanhar o cumprimento dessas obrigações e avaliar periodicamente os riscos associados aos serviços terceirizados.

7. Controlar o compartilhamento

A entrega de imagens deve ter finalidade e fundamento jurídico, além de se limitar ao trecho necessário. Além disso, solicitações de autoridades, seguradoras ou pessoas filmadas precisam seguir procedimentos próprios, com proteção dos demais envolvidos.

8. Definir prazo de guarda e eliminar as imagens

O prazo de armazenamento deve ser justificado conforme a finalidade do monitoramento. A LGPD não estabelece um período geral de retenção para imagens de câmeras de segurança, e a capacidade técnica do sistema, por si só, não deve determinar quanto tempo os registros devem ser mantidos. É preciso encontrar um equilíbrio. Ao fim do prazo definido, as imagens devem ser eliminadas. Trechos relacionados a uma ocorrência só podem ser preservados separadamente, com justificativa, acesso restrito e revisão da necessidade de conservação.

9. Testar o funcionamento e avaliar recursos adicionais

O videomonitoramento pode envolver riscos à privacidade, especialmente quando ocorre de forma sistemática, abrange um grande número de pessoas ou utiliza tecnologias capazes de ampliar a identificação e o acompanhamento dos indivíduos. Nesses casos, a empresa deve avaliar a necessidade de elaborar um Relatório de Impacto à Proteção de Dados Pessoais (RIPD), documento que descreve as operações de tratamento, identifica possíveis riscos aos direitos e às liberdades dos titulares e apresenta medidas para preveni-los ou mitigá-los. A avaliação também deve considerar os locais monitorados, as tecnologias utilizadas, as finalidades da captação e as condições de acesso e armazenamento das imagens. A depender do contexto, a ANPD pode solicitar a elaboração do relatório.

10. Preparar-se para incidentes

A organização precisa ter um fluxo para conter acessos indevidos, preservar evidências, avaliar os efeitos sobre as pessoas e corrigir a causa. Incidentes de segurança que possam gerar risco ou dano relevante aos titulares devem ser comunicados à ANPD e às pessoas afetadas, conforme os prazos e procedimentos previstos na regulamentação aplicável.

"A Axis recomenda que as empresas revisem periodicamente as câmeras, os ângulos, os usuários, os aplicativos e os fornecedores envolvidos. A revisão também deve considerar mudanças de função, desligamentos e alterações nos serviços contratados. A política de videomonitoramento precisa estabelecer responsabilidades e orientar as equipes sobre consulta, exportação, compartilhamento, guarda e eliminação das imagens.", afirma Mariana Dessotti, CEO & Founder da Axis AI & Privacy Governance.

"A segurança patrimonial costuma conduzir a operação das câmeras, mas essa atividade exige a participação de diferentes especialidades. Definir o que será filmado, quem poderá acessar as imagens e em quais situações elas poderão ser compartilhadas envolve questões tecnológicas, jurídicas e de proteção de dados. A atuação conjunta dessas equipes permite avaliar os riscos e estabelecer procedimentos que atendam às necessidades de segurança da empresa e às exigências da LGPD", afirma Fernando Nery, membro do conselho da Axis AI & Privacy Governance.

Mesmo quando há apenas transmissão ao vivo, sem gravação, o videomonitoramento configura tratamento de dados pessoais sempre que permite identificar pessoas. Por isso, a gestão dessas imagens deve fazer parte da estrutura contínua de governança de privacidade da empresa, com responsabilidades definidas, controles documentados e procedimentos que possam ser demonstrados na operação.

A regra dos 180 dias: como o prazo semestral do CFM trava o avanço da saúde digital

Thamires Cappello (*)

A telemedicina ampliou o acesso à saúde no Brasil ao aproximar pacientes e especialistas, encurtar distâncias e facilitar a continuidade do cuidado

Segundo a pesquisa TIC Saúde 2025, conduzida pelo Cetic.br, 28% dos estabelecimentos de saúde conectados à internet ofereciam teleconsultas, ante 23% em 2024.

Com a expansão dessa modalidade, é importante avaliar se as regras que orientam sua prática acompanham as necessidades dos pacientes. Um exemplo é a Resolução CFM nº 2.314/2022, do Conselho Federal de Medicina, que exige consultas presenciais a cada 180 dias, no máximo, para pacientes com doenças crônicas ou que necessitem de acompanhamento prolongado por telemedicina.

A preocupação com a segurança assistencial é legítima e o exame físico continua indispensável em diversas situações. Mas será que todos os pacientes precisam seguir a mesma periodicidade, independentemente de sua condição clínica?

Doenças crônicas envolvem cenários distintos: um paciente com hipertensão ou diabetes controlados, metas terapêuticas estáveis e monitoramento regular apresenta demandas diferentes das de alguém em ajuste medicamentoso ou com comorbidades instáveis, por exemplo. Uma revisão de estudos publicada em 2022 no BMC Primary Care identificou resultados semelhantes aos do atendimento presencial no acompanhamento remoto de diabetes, hipertensão e colesterol elevado. Embora os autores ressaltem a necessidade de mais pesquisas, os resultados indicam que a telemedicina pode ser uma alternativa adequada em determinadas condições clínicas.

Ao estabelecer um prazo fixo, a norma pode criar barreiras que nem sempre correspondem às necessidades clínicas. Para quem vive longe dos centros especializados, uma consulta presencial pode envolver deslocamentos, perda de dias de trabalho e custos adicionais. Quando não há indicação clínica para esse retorno, a exigência pode dificultar a continuidade do tratamento em vez de contribuir para sua qualidade.

Claro que, para garantir a segurança do paciente, a decisão final sobre o formato do atendimento deve ser sempre do médico. A Lei nº 14.510/2022, que regulamentou a telessaúde meses após a publicação da resolução do CFM, também reconhece a autonomia do profissional de saúde para decidir sobre o atendimento remoto e indicar a modalidade presencial quando necessário. A legislação garante ainda ao paciente o direito de solicitar atendimento presencial. Assim, se avaliar que o quadro clínico exige um exame físico ou outro tipo de acompanhamento presencial, o médico tem respaldo legal para encaminhar o paciente. A mesma legislação também assegura ao paciente o direito de solicitar atendimento presencial sempre que desejar.

Nesse contexto, a segurança clínica deve estar associada à adequação do acompanhamento às necessidades de cada paciente, e não apenas à uniformização de prazos. A avaliação médica, considerando a evolução do quadro e os riscos envolvidos, deve orientar a frequência e a modalidade das consultas.

Portanto, rever a obrigatoriedade do prazo de 180 dias e transformá-lo em uma recomendação permitiria maior flexibilidade no acompanhamento, sem abrir mão da avaliação presencial quando necessária. Em um país de dimensões continentais e com distribuição desigual de especialistas, a saúde digital precisa de regras que protejam os pacientes sem criar obstáculos desnecessários. Afinal, o cuidado deve ser guiado pelas necessidades de quem recebe a assistência, não pela rigidez de um calendário.

(*) Doutora em Ciências da Saúde e Saúde Pública pela USP. Mestre em Direito pela PUC/SP. Pesquisadora no Centro de Direito Sanitário da USP.

Condomínios podem ter de indenizar moradores por falhas no controle de acesso, decide STJ

Uma falha na portaria levou um condomínio do Rio de Janeiro a ser condenado ao pagamento de aproximadamente R$ 36 mil em indenizações a moradores que tiveram o apartamento furtado. A decisão foi mantida por unanimidade pela Terceira Turma do Superior Tribunal de Justiça (STJ), no julgamento do Recurso Especial 2.264.505/RJ, realizado em setembro de 2026 e divulgado pelo tribunal em novembro. O caso envolveu a entrada de criminosos no edifício sem a devida verificação de identidade e autorização dos moradores, evidenciando os riscos jurídicos relacionados à negligência nos procedimentos de segurança condominial.

A condenação compreendeu R$ 24 mil por danos morais e aproximadamente R$ 12 mil por danos materiais, com fundamento nos artigos 186, 927 e 932, inciso III, do Código Civil. O entendimento, porém, não estabelece que os condomínios devam garantir que nenhum crime aconteça em suas dependências. A responsabilização pode ocorrer quando uma conduta negligente ou imprudente de um funcionário contribui para a prática criminosa, considerando as circunstâncias e as provas de cada caso.

Para o advogado Dr. Tony Santtana, o episódio demonstra que a segurança de um condomínio não depende apenas dos equipamentos instalados, mas também da forma como os procedimentos são executados. "Não adianta investir em câmeras, portões eletrônicos e sistemas modernos se o controle de entrada não funciona adequadamente. A identificação de visitantes e a autorização dos moradores precisam ser respeitadas. Quando a falha de um funcionário facilita a prática de um crime, o condomínio pode enfrentar consequências jurídicas e financeiras", afirma. Diante desse cenário, síndicos e administradoras precisam revisar os protocolos de acesso, orientar os funcionários e acompanhar o funcionamento dos sistemas de monitoramento. A existência de equipamentos de segurança, por si só, não afasta a possibilidade de responsabilização. Mais do que proteger o patrimônio dos moradores, o cumprimento desses procedimentos também é uma forma de reduzir riscos e evitar problemas jurídicos para a administração condominial.