WHITE PAPER

Privacidade no monitoramento

Ferramentas e tecnologias para proteção da privacidade

Dezembro 2023

AXIS COMMUNICATIONS

Resumo

As soluções de monitoramento devem cumprir as regulamentações de privacidade locais, regionais ou outras regulamentações de privacidade aplicáveis que imponham restrições à coleta de dados de identificação pessoal.

Existem diversas ferramentas e tecnologias para ajudar a proteger a privacidade das pessoas no monitoramento.

- O **mascaramento dinâmico** torna as pessoas ou veículos anônimos no vídeo em tempo real. O aplicativo de analíticos AXIS Live Privacy Shield oferece mascaramento dinâmico baseado em IA em algumas câmeras para detectar e mascarar seres humanos ou placas de licença. Ele também oferece mascaramento dinâmico baseado em movimento em todas as câmeras compatíveis permitindo mascarar todos os objetos em movimento.
- O **mascaramento estático** oculta uma área selecionada aplicando uma máscara permanente em todos os vídeos ao vivo e gravados. O recurso está disponível por padrão nos produtos de vídeo em rede Axis e é ideal para cenas internas ou externas onde há determinadas áreas que você não tem permissão para monitorar.
- A **edição de vídeo** no software de gerenciamento de vídeo (VMS) pode ser usada, por exemplo, quando você precisa exportar vídeos para uma investigação forense, e ao mesmo tempo, proteger a privacidade dos espectadores na filmagem.
- **Monitoramento não visual**

  As **câmeras térmicas** geram imagens com base no calor emitido pelos objetos. São capturadas apenas formas, sem detalhes pessoais.

  Os **radares no monitoramento** fornecem detecção sem gerar detalhes de identificação pessoal.
- Os **analíticos** baseados em vídeo ou áudio podem ser usados para monitorar uma cena e desencadear ações quando algo se destaca. Os analíticos também podem visualizar dados em painéis sem a necessidade de armazenar nenhuma gravação.

O proprietário de um sistema de monitoramento é responsável por garantir a conformidade com os regulamentos de privacidade.

Sumário

1 Introdução

Existem várias opções de como proteger a privacidade no monitoramento. Você pode, por exemplo, bloquear áreas na exibição da câmera, colocar máscaras em pessoas no vídeo ou usar tecnologias não visuais para o seu monitoramento.

Este white paper apresenta as principais ferramentas e tecnologias para abordar questões de privacidade durante a captura, gravação, visualização e exportação de vídeos de monitoramento.

2 Cenário

O monitoramento em áreas públicas está sendo mais aceito à medida que os cidadãos compreendem como isso pode aumentar a sua segurança e proteção. Embora a privacidade sempre tenha sido uma prioridade no setor de monitoramento, a consciência das pessoas sobre os seus direitos foi aumentada por iniciativas como o GDPR (Regulamento Geral de Proteção de Dados) na Europa e a FISMA (Lei Federal de Gerenciamento de Segurança da Informação) nos EUA.

Tanto na esfera pública como na privada, existem regras e regulações dos governos locais e regionais e dos sindicatos referentes ao videomonitoramento e à privacidade. A regulação existe para proteger os direitos humanos, preservando o direito das pessoas à privacidade. Dessa forma, estabelece controles que devem ser implementados sobre a captura, o armazenamento e o compartilhamento de dados de vídeo.

É sempre o proprietário de um sistema de monitoramento o responsável por garantir que o seu monitoramento cumpre todos os regulamentos de privacidade locais e internacionais aplicáveis. No entanto, fabricantes e fornecedores podem ajudar os seus clientes a manterem-se informados sobre as melhores práticas de monitoramento. Isso abrange como utilizar os dados coletados de forma correta e ética e tomar as medidas necessárias para cumprir os regulamentos.

3 Mascaramento em video

Existem várias técnicas para ocultar áreas selecionadas ou tornar anônimas pessoas em vídeos de monitoramento.

Para todos os tipos de mascaramento, você pode escolher entre máscara com cor sólida ou mosaico (pixelada). O mascaramento com cores oferece o máximo de proteção de privacidade ao mesmo tempo que permite a você ver o movimento. O mascaramento com mosaico mostra objetos ou seres humanos

em movimento em resolução muito baixa, permitindo uma melhor distinção das formas por meio das cores reais do objeto.

Mascaramento com cores e mascaramento com mosaico.

3.1 Mascaramento dinâmico

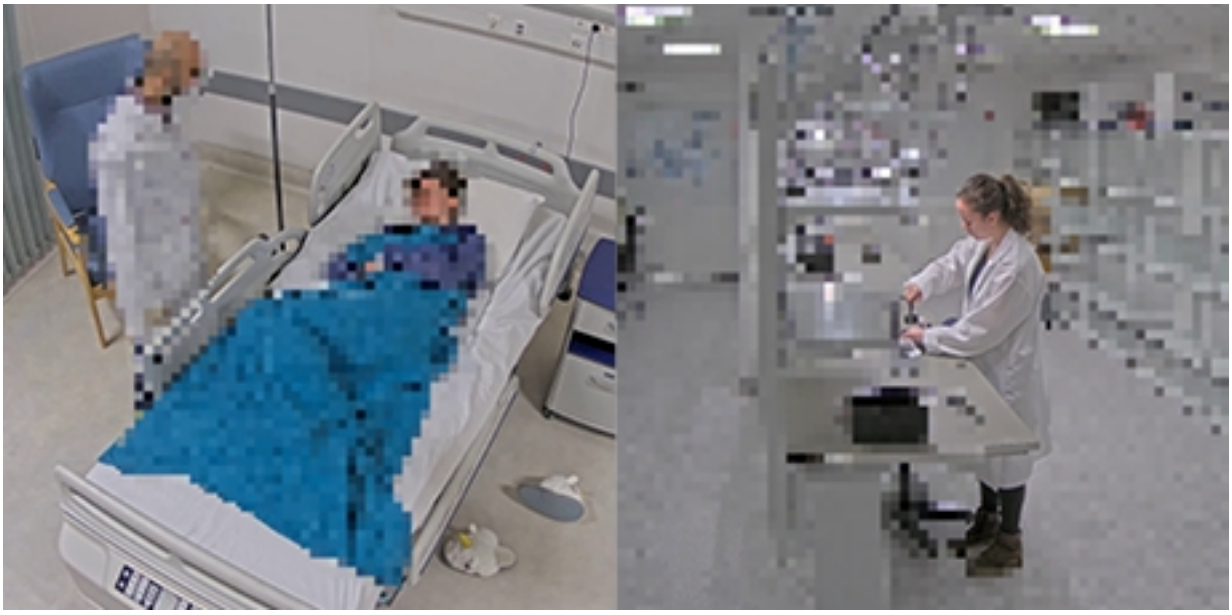
Com essa técnica, os analíticos de vídeo automaticamente tornam anônimas as pessoas no vídeo. Isso acontece em tempo real à medida que os analíticos monitoram as ações e os movimentos na cena.

O aplicativo de analíticos baseado em borda AXIS Live Privacy Shield oferece mascaramento dinâmico baseado em IA nas câmeras visuais.

3.1.1 Mascaramento baseado em IA

Esse mascaramento tem suporte em algumas câmeras que têm uma unidade de processamento de aprendizado profundo (DLPU). Com o mascaramento baseado em IA, o aplicativo analisa o vídeo ao vivo para detectar seres humanos ou placas de licença. Você pode optar por mascarar seres humanos (em

movimento e parados), rostos ou placas de licença. Em vez disso, o método de mascaramento também pode ser invertido para mascarar o plano de fundo.



Mascaramento de humanos e do plano de fundo no AXIS Live Privacy Shield.

O AXIS Live Privacy Shield permite o mascaramento dinâmico baseado em IA em até 10 quadros por segundo. É ideal para cenas internas e externas de curta distância em locais como fábricas, hospitais, lares para idosos, hotéis, escolas, escritórios e lojas.

Com o mascaramento baseado em IA, o mascaramento permanecerá mesmo quando as pessoas ficarem imóveis por longos períodos.

3.1.2 Streams com e sem máscara

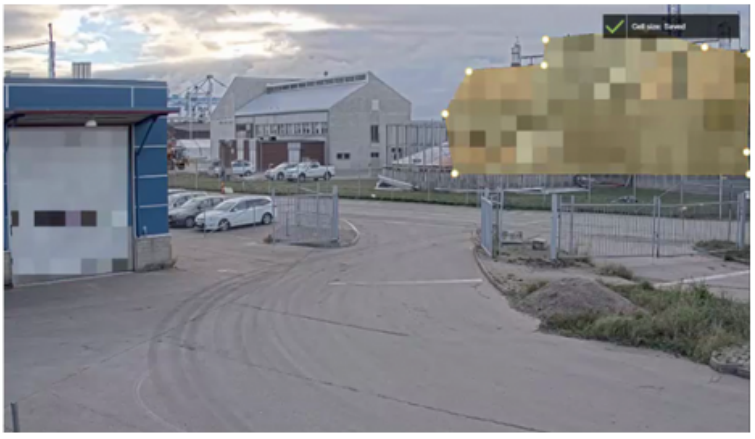
O mascaramento com o AXIS Live Privacy Shield é permanente, o que significa que ele não pode ser removido do vídeo após a gravação. No entanto, você pode optar por fazer com que o aplicativo forneça um fluxo de vídeo com mascaramento e, simultaneamente, um fluxo diferente sem mascaramento. Dependendo do VMS, você pode configurar os direitos de acesso dos streams.

Assim, você pode manter um fluxo sem mascaramento que somente pessoas autorizadas podem visualizar. Se as identidades das pessoas capturadas nas filmagens sejam essenciais para uma investigação, nesse caso, existe uma maneira de recuperar essas informações. Manter fluxos de streams paralelos não só protege o direito à privacidade dos indivíduos, mas também abrange as obrigações do proprietário do monitoramento de manter as pessoas seguras, especialmente em espaços públicos abertos.

3.2 Mascaramento estático

O mascaramento de privacidade estático é ideal para cenas internas ou externas onde existem áreas fixas que você não tem permissão para monitorar. Esse mascaramento oculta uma área selecionada aplicando uma máscara permanente (opaca ou mosaico) nos vídeos ao vivo e gravados. Com uma máscara de mosaico, a área é mostrada em resolução muito baixa para que você possa ver a atividade sem identificar detalhes pessoais.

O mascaramento de privacidade estático é um atributo padrão dos produtos de vídeo em rede Axis. Ele pode ser combinado com o mascaramento dinâmico do AXIS Live Privacy Shield.



Mascaramento de privacidade estático usando uma máscara de mosaico poligonal para bloquear permanentemente o monitoramento de um edifício.

O mascaramento de áreas específicas para evitar monitoramento não intencional tem valor especialmente com câmeras PTZ (pan-tilt-zoom), devido a sua cobertura de longa distância e área ampla. Em uma câmera PTZ, o mascaramento de privacidade estático é estabelecido no sistema de coordenadas da câmera. Como resultado, o mascaramento permanece na mesma área da cena, até quando o campo de visão é alterado.

4 Edição de vídeo

Ao compartilhar gravações de vídeo, você deve cumprir todos os regulamentos aplicáveis que protegem a privacidade dos espectadores. Uma ferramenta de edição de vídeo no AXIS Camera Station permite mascarar facilmente indivíduos ou áreas em uma cena que não são interessantes para uma investigação. Você pode, por exemplo, mascarar apenas objetos em movimento selecionados ou mascarar todos os objetos parados e em movimento, exceto pessoas de interesse.

Observe que a edição de vídeo não pode ser usada em vídeos ao vivo.

5 Monitoramento não visual

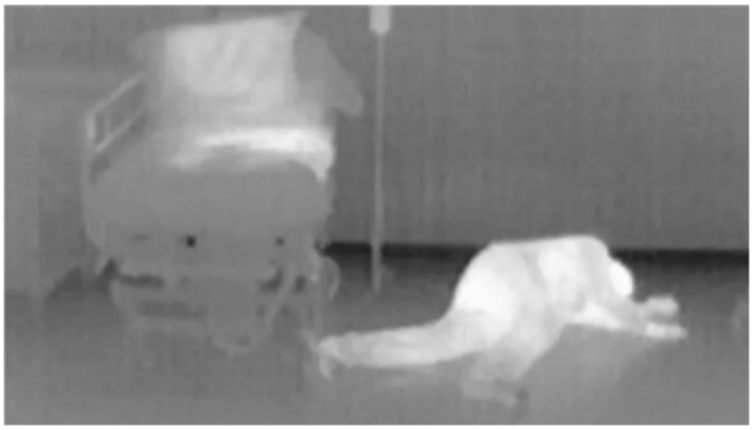
Em alguns casos, a privacidade no monitoramento é melhor garantida utilizando detectores não visuais em vez de câmaras comuns. Estas soluções funcionam em qualquer clima e qualquer luz.

5.1 Imagem térmica

As câmeras térmicas detectam calor em vez de luz visível. Elas criam uma imagem com base no calor que irradia dos objetos que estão dentro do campo de "visão" da câmera. Isso permite o monitoramento remoto sem coletar dados pessoais. Somente formas – em movimento ou paradas – são capturadas.

Câmeras térmicas com analíticos de detecção de movimento integrados são úteis em ambientes com altas exigências de privacidade. Em locais como instalações de saúde ou lares para idosos, as câmeras térmicas

protegem a privacidade pessoal e alertam rapidamente a equipe sobre movimentos inesperados. Se um paciente cair ou precisar de assistência médica, a equipe poderá responder imediatamente.



As câmeras térmicas permitem o monitoramento remoto sem detalhes pessoais identificáveis.

5.2 Radar

Um radar fornece monitoramento com total privacidade porque utiliza tecnologia de radar em vez de tecnologia de vídeo.

Um radar funciona transmitindo ondas de rádio e recebendo e analisando as mesmas ondas refletidas em objetos em seu campo de detecção. A tecnologia de radar com análise detecta movimento e dispara alarmes sem coletar dados pessoais. É ideal para detectar intrusos em espaços abertos. O radar pode então alertar automaticamente a segurança e ativar alto-falantes para dissuasão.

5.3 Análise

Os analíticos de vídeo e áudio podem ser usados para ajudar a monitorar uma cena em tempo real e reagir quando algo se destacar. Os analíticos geram metadados, que podem ser usados para compreensão da cena sem a necessidade de acessar os streams de vídeo ou áudio, nem de armazenar as gravações. Os dados podem ser visualizados em planilhas e painéis, ou acionar alarmes em tempo real. Isso pode ajudar a resolver questões de privacidade relacionadas aos dados pessoais. Os analíticos de áudio podem acionar alarmes quando um microfone capta sons associados, por exemplo, pessoas gritando, vidros quebrando ou outros sons anormais.

6 Proteção de dados

A proteção de dados está fora do escopo deste documento. No entanto, a forma como os dados de videomonitoramento são tratados é um aspecto importante da proteção da privacidade. Consulte *www.axis.com/about-axis/cybersecurity* para obter mais informações.

Sobre a Axis Communications

A Axis torna possível um mundo mais inteligente e seguro criando soluções para melhorar a segurança e o desempenho dos negócios. Como empresa de tecnologia de rede e líder do setor, a Axis oferece soluções em videomonitoramento, controle de acesso, intercomunicação e áudio. Nossas soluções são aprimoradas por aplicativos de análise inteligentes e apoiados por treinamento de alta qualidade.

A Axis tem cerca de 4.000 funcionários dedicados em mais de 50 países e colabora com parceiros de tecnologia e integração de sistemas em todo o mundo para fornecer soluções aos clientes. A Axis foi fundada em 1984 e tem sede em Lund, Suécia