DOCUMENTO TÉCNICO

Privacidad en la vigilancia

Herramientas y tecnologías para preservar la privacidad

Diciembre 2023

AXIS COMMUNICATIONS

Resumen

Las soluciones de vigilancia deben cumplir las normas locales, regionales y de otro tipo en materia de privacidad que planteen restricciones a la recopilación de datos que permitan la identificación de personas.

Hay varias herramientas y tecnologías disponibles que contribuyen a proteger la privacidad de las personas en la vigilancia.

- El **enmascaramiento dinámico** anonimiza a personas o vehículos en las imágenes de vídeo en tiempo real. La aplicación de analíticas AXIS Live Privacy Shield ofrece enmascaramiento dinámico basado en la IA en cámaras específicas para detectar y enmascarar personas o matrículas. Asimismo, ofrece enmascaramiento dinámico basado en el movimiento en todas las cámaras compatibles para enmascarar todos los objetos en movimiento.
- El **enmascaramiento estático** oculta una zona seleccionada aplicando una máscara permanente en todas las imágenes de vídeo en directo y grabadas. Está disponible como función estándar en los productos de vídeo en red de Axis y es una opción perfecta para las escenas de interiores o exteriores en las que hay zonas fijas que no tiene autorización para supervisar.
- La **edición de vídeo** en software de gestión de vídeo puede usarse cuando es necesario exportar vídeo, por ejemplo, para una investigación forense, preservando al mismo tiempo la privacidad de los transeúntes que aparecen en las imágenes.
- **Vigilancia no visual**

  Las cámaras térmicas crean imágenes basadas en el calor que irradian los objetos. Solo se capturan las formas, sin ningún detalle personal.

  Los radares utilizados en la vigilancia detectan sin generar ningún detalle que permita la identificación de personas.
- Las **analíticas** basadas en vídeo o audio pueden servir para supervisar una escena y activar acciones cuando se produce alguna situación destacada. Las analíticas también pueden visualizar datos en paneles de mando sin necesidad de almacenar ninguna grabación.

El propietario de un sistema de vigilancia es el responsable de garantizar que se cumplan los reglamentos sobre privacidad.

Índice

1 Introducción

Existen diversas opciones sobre cómo proteger la privacidad en la vigilancia. Por ejemplo, se pueden bloquear zonas de la vista de cámara, aplicar una máscara a personas que aparecen en el vídeo o utilizar tecnologías no visuales para la vigilancia.

En este documento técnico se exponen las principales herramientas y tecnologías para abordar los problemas relacionados con la privacidad durante la captura, grabación, visionado y exportación de imágenes de videovigilancia.

2 Contexto

La vigilancia en espacios públicos está cada vez más aceptada a medida que los ciudadanos comienzan a comprender que puede aumentar su seguridad y protección. Si bien la privacidad ha sido siempre prioritaria en el sector de la vigilancia, la sensibilización de las personas con respecto a sus derechos ha aumentado gracias a iniciativas como el RGPD (Reglamento General de Protección de Datos) en Europa y la FISMA (Ley federal de gestión de la seguridad de la información) en EE. UU.

Tanto en la esfera pública como en la privada, existen normas y reglamentos dictados por los gobiernos y sindicatos locales y regionales en relación con la videovigilancia y la privacidad. La normativa tiene por objeto proteger los derechos humanos mediante la preservación del derecho a la privacidad de las personas. Por consiguiente, establece medidas de control que deben implantarse en torno a la captura, el almacenamiento y el uso compartido de los datos de vídeo.

Es siempre el propietario de un sistema de vigilancia quien tiene la responsabilidad de garantizar que su actividad sea conforme a todos los reglamentos locales e internacionales aplicables en materia de privacidad. Sin embargo, los fabricantes y proveedores pueden ayudar a sus clientes a mantenerse al día de las prácticas recomendadas de vigilancia. Aquí se incluye cómo utilizar los datos recopilados de una forma correcta y ética, y cómo adoptar los pasos necesarios para cumplir con la normativa.

3 Enmascaramiento en vídeo

Existen diversas técnicas para ocultar áreas seleccionadas o anonimizar a personas en secuencias de videovigilancia.

Con independencia del tipo de enmascaramiento, puede elegir entre un enmascaramiento de color sólido o mosaico (pixelado). El enmascaramiento de color proporciona la máxima protección de privacidad y permite

ver los movimientos. El enmascaramiento de mosaico muestra objetos o personas en movimiento a muy baja resolución y permite distinguir mejor las formas mediante los colores reales del objeto.

Enmascaramiento de color y enmascaramiento de mosaico.

3.1 Enmascaramiento dinámico

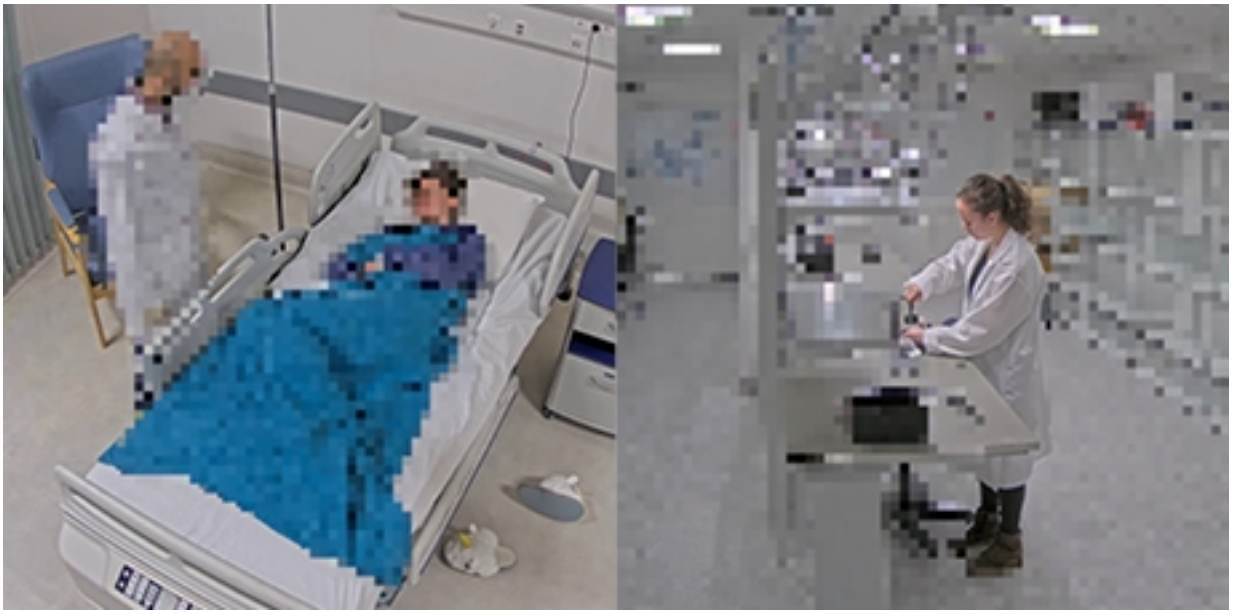
Con esta técnica, las analíticas de vídeo anonimizan de forma automática a las personas que aparecen en el vídeo. Esto ocurre en tiempo real, mientras las analíticas supervisan las acciones y los movimientos que se producen en la escena.

La aplicación de analíticas basada en el extremo AXIS Live Privacy Shield ofrece enmascaramiento dinámico basado en IA en las cámaras visuales.

3.1.1 Enmascaramiento basado en IA

Esta función es posible en cámaras específicas que poseen una unidad de procesamiento de aprendizaje profundo (DLPU, por sus siglas en inglés). En el enmascaramiento basado en IA, la aplicación analiza secuencias de vídeo en directo para detectar personas o matrículas. Puede seleccionar si desea aplicar

el enmascaramiento solo a personas (en movimiento y estáticas), rostros, o matrículas. El método de enmascaramiento se puede invertir para enmascarar el fondo.



Enmascaramiento de personas y del fondo en AXIS Live Privacy Shield.

AXIS Live Privacy Shield admite el enmascaramiento dinámico basado en IA de hasta 10 fotogramas por segundo. Resulta apropiado para escenas de rango cercano en interiores y exteriores, como fábricas, hospitales, residencias de ancianos, hoteles, escuelas, oficinas y comercios.

Con el enmascaramiento basado en IA, la máscara se mantendrá también cuando las personas permanezcan inmóviles de forma prolongada.

3.1.2 Flujos de transmisión con y sin máscara

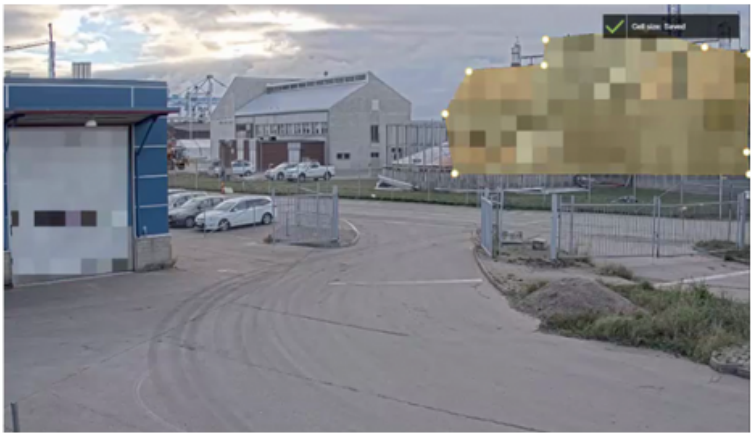
El enmascaramiento con AXIS Live Privacy Shield es permanente en tanto que no se puede quitar de las imágenes de vídeo después de grabar. No obstante, puede seleccionar la posibilidad de que la aplicación genere un flujo de transmisión de vídeo con máscara y, al mismo tiempo, un flujo de transmisión independiente sin enmascaramiento. En función del software de gestión de vídeo (VMS) utilizado, puede configurar los derechos de acceso de los flujos de transmisión.

De este modo, puede mantener un flujo de transmisión sin máscara que solo puede ver el personal autorizado. En el supuesto de que la identidad de las personas grabadas sea determinante para una investigación, existe una forma de recuperar dicha información. Conservar flujos de transmisión paralelos no solo protege el derecho a la privacidad de las personas, sino que también cubre las obligaciones del propietario del sistema de vigilancia de preservar la seguridad de las personas, sobre todo en espacios abiertos públicos.

3.2 Enmascaramiento estático

El enmascaramiento estático de la privacidad resulta idóneo para escenas de interior o exterior en las que hay áreas cuya supervisión no está permitida. Oculta un área seleccionada aplicando una máscara (opaca o de mosaico) permanente en los vídeos en vivo y grabados. Con una máscara de mosaico, el área se representa con una resolución muy baja para que pueda ver la actividad sin detalles que permitan la identificación de personas.

El enmascaramiento estático de la privacidad es una característica estándar de los productos de vídeo de red de Axis. Se puede combinar con el enmascaramiento dinámico de AXIS Live Privacy Shield.



El enmascaramiento estático de la privacidad utiliza una máscara de mosaico poligonal para impedir de forma permanente que se pueda supervisar un edificio.

El enmascaramiento de zonas específicas para evitar una vigilancia accidental resulta especialmente valioso con las cámaras PTZ (panorámica-inclinación-zoom), dada su cobertura de larga distancia y de área extensa. En una cámara PTZ, el enmascaramiento estático de la privacidad está incorporado en el sistema de coordenadas de la cámara. Por este motivo, el enmascaramiento se mantiene en la misma área de la escena incluso cuando cambia el campo de visión.

4 Redacción de vídeo

Al compartir grabaciones de vídeo, tiene que cumplir con cualquier normativa aplicable que proteja la privacidad de los transeúntes. Una herramienta de edición de vídeo de AXIS Camera Station le permite enmascarar fácilmente personas o áreas en una escena que no es de interés para una investigación. Por ejemplo, puede enmascarar solo objetos móviles seleccionados o enmascarar todos los objetos estáticos y móviles excepto las personas de interés.

Tenga en cuenta que la edición de vídeo no está disponible en el vídeo en directo.

5 Vigilancia no visual

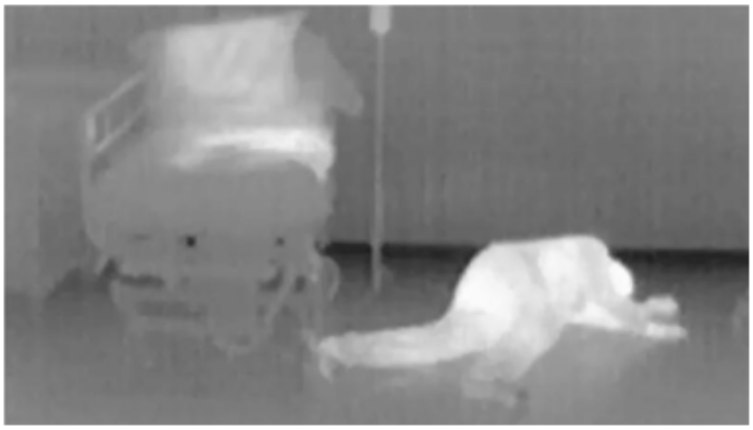
En algunos casos, la mejor forma de garantizar la privacidad en la vigilancia es mediante el uso de detectores no visuales en lugar de cámaras normales. Estas soluciones funcionan con toda clase de condiciones meteorológicas y luz.

5.1 Imágenes térmicas

Las cámaras térmicas detectan el calor en lugar de la luz visible. Crean una imagen basada en el calor que irradian los objetos situados en el campo de visión de la cámara. Esto permite vigilar a distancia sin recopilar datos personales. Solo se capturan formas (en movimiento o estáticas).

Las cámaras térmicas con analíticas de detección de movimiento integradas resultan útiles en entornos donde la exigencia de privacidad es alta. En lugares como centros sanitarios o residencias de ancianos,

las cámaras térmicas protegen la intimidad personal y alertan con rapidez al personal de movimientos inesperados. Si un paciente se cae o precisa asistencia médica, el personal puede actuar con rapidez.



Las cámaras térmicas permiten la vigilancia a distancia sin detalles que permitan la identificación de personas.

5.2 Radar

Un radar realiza la vigilancia con una privacidad total porque utiliza tecnología de radar en lugar de la tecnología de vídeo.

Un radar funciona mediante la transmisión de ondas de radio y la recepción y el análisis de las mismas ondas rebotadas desde los objetos que se encuentran en su campo de detección. La tecnología de radar con analíticas detecta movimiento y activa alarmas sin recopilar datos personales. Resulta idónea para la detección de intrusos en amplios espacios abiertos. Posteriormente, el radar puede avisar automáticamente a los servicios de seguridad y activar altavoces a modo de disuasión.

5.3 Analítica

Las analíticas de vídeo y audio pueden utilizarse para supervisar una escena en tiempo real y reaccionar cuando se produce alguna situación destacada. Las analíticas generan metadatos, que pueden servir para comprender una escena sin necesidad de acceder a flujos de transmisión de vídeo o audio ni almacenar las grabaciones. Los datos se pueden visionar en hojas de cálculo y paneles de mando, o activar alarmas en tiempo real. De esta forma, se pueden abordar los problemas de privacidad relacionados con los datos personales. Las analíticas de audio pueden activar alarmas cuando un micrófono captura sonidos relacionados, por ejemplo, con gritos de personas, roturas de cristales u otros sonidos anómalos.

6 Protección de datos

La protección de datos no se aborda en este documento. No obstante, el manejo de los datos de videovigilancia es un aspecto importante de la protección de la privacidad. Para más información, consulte *https://www.axis.com/es-es/about-axis/cybersecurity*.

Acerca de Axis Communications

Axis contribuye a crear un mundo más inteligente y seguro a través de soluciones para mejorar la seguridad y el rendimiento empresarial. Como empresa de tecnología de red y líder del sector, Axis ofrece soluciones de videovigilancia, control de acceso y sistemas de audio e intercomunicación. Se ven reforzadas por aplicaciones de análisis inteligentes y respaldadas por formación de alta calidad.

Axis tiene alrededor de 4000 empleados dedicados en más de 50 países y colabora con socios de integración de sistemas y tecnología en todo el mundo para ofrece soluciones personalizadas. Axis se fundó en 1984 y la sede está en Lund, Suecia