



NOTICIA DOCTRINAL

TRIBUNAL PERICIAL

EL DIRECTOR DE SEGURIDAD

LA VIDEO VIGILANCIA DOMÉSTICA EN LOS TRIBUNALES

Reto Operativo y Jurídico de las Cámaras IP no Homologadas



Autor: Manuel David Moreno Morgado

Especialidad: Dirección de Seguridad Privada – Perito Judicial

RESUMEN EJECUTIVO:

La democratización de los sistemas de videovigilancia mediante cámaras IP domésticas (*Plug & Play*) ha transformado el acervo probatorio en los tribunales. Sin embargo, evaluar estos sistemas bajo el prisma de las instalaciones profesionales de Circuito Cerrado de Televisión (CCTV) genera impugnaciones infundadas.

En este artículo analizamos, desde la óptica de la Dirección de Seguridad Privada, la operativa de extracción en aplicaciones comerciales (ej. TAPO) y desmontamos la falacia de exigir protocolos de cadena de custodia policial a ciudadanos particulares, al amparo de la consolidada doctrina del Tribunal Supremo.

1. El Paradigma de la Seguridad "Plug & Play" y la Prueba Judicial

En la práctica judicial contemporánea, una gran parte de los ilícitos penales, conflictos laborales o disputas civiles se resuelven gracias a grabaciones de vídeo. Como expertos en Seguridad Privada, estamos acostumbrados a gestionar sistemas de CCTV profesionales, sujetos a la normativa de Seguridad Privada, con grabadores físicos dedicados (NVR/DVR) y protocolos de extracción tasados.

El conflicto actual en los juzgados surge por la proliferación de cámaras IP de consumo (marcas como TAPO, Xiaomi, Ring, etc.). Estos dispositivos, al no estar clasificados bajo los grados de seguridad de la norma **UNE-EN 50131**, operan con lógicas de red y almacenamiento completamente distintas. Cuando la contraparte impugna un vídeo de estas cámaras alegando bajadas de calidad, cortes de audio o formatos dispares, a menudo confunde la **respuesta operativa programada del sistema** con una manipulación maliciosa.

Es nuestro deber, como peritos en Dirección de Seguridad, aclarar a Sus Señorías la realidad de estos sistemas.

2. La Operativa de Exportación y la Gestión del Ancho de Banda

Para comprender las supuestas "anomalías" de estos vídeos, debemos abandonar el análisis forense purista y centrarnos en la **arquitectura del sistema**.

Cuando un usuario exporta un vídeo desde la App de su móvil, no está realizando un volcado físico de un disco duro en una Central Receptora, sino capturando un flujo de transmisión (*streaming*) desde la nube o la tarjeta SD integrada (*Edge Storage*).



NOTICIA DOCTRINAL

TRIBUNAL PERICIAL

EL DIRECTOR DE SEGURIDAD

LA VIDEO VIGILANCIA DOMÉSTICA EN LOS TRIBUNALES

Reto Operativo y Jurídico de las Cámaras IP no Homologadas



Esta operativa condiciona inevitablemente el archivo resultante:

- **Disparidad de Contenedores:** El archivo final depende del teléfono del usuario, no de la cámara. Un dispositivo Android encapsulará el flujo en un .MP4, mientras que un iPhone forzará la creación de un contenedor .MOV con metadatos de Apple. Operativamente, esto es un comportamiento estándar del *software* comercial, no un indicio de edición.
- **Gestión de Red y Caída de Frames:** A diferencia de un CCTV profesional cableado, las cámaras Wi-Fi domésticas priorizan la **continuidad de la grabación sobre la calidad**. Ante una fluctuación de red o saturación del ancho de banda, el sistema está programado para bajar automáticamente los fotogramas por segundo (FPS) o el *bitrate*. No hay manipulación, hay un protocolo de supervivencia de la transmisión.
- **El "Falso Corte" de Audio (AGC):** Para evitar la saturación del canal, estos dispositivos aplican un Control Automático de Ganancia. Ante un ruido ambiental fuerte, el micrófono reduce drásticamente su sensibilidad. Lo que en un juicio se intenta vender como un "corte manual de audio para ocultar una conversación", en términos de seguridad electrónica es simplemente la actuación del limitador acústico del dispositivo.

3. La Doctrina del Tribunal Supremo y la Realidad del Ciudadano

Es alarmantemente habitual observar contra-informes que exigen la nulidad de estas grabaciones ciudadanas alegando incumplimientos de estándares como la **ISO/IEC 27037** (directrices para la identificación y recopilación de evidencia digital).

Desde la Dirección de Seguridad Privada, debemos denunciar esta falacia: **los ciudadanos no son First Responders ni vigilantes de seguridad formados**.

Exigir a un particular que, en una situación de estrés tras sufrir un delito, aplique protocolos de cadena de custodia profesional o calcule algoritmos *Hash* al exportar el vídeo desde su sofá, es un despropósito operativo y jurídico.

La jurisprudencia española avala esta flexibilización. La consolidada **STS 300/2015, de 19 de mayo** (reiterada en la **STS 754/2015** de la Sala de lo Penal), establece que la prueba digital aportada por particulares es válida por sí misma. Ahora bien, **si es impugnada, quien la aporta debe demostrar su autenticidad**.

Y es aquí donde nuestra pericial cobra sentido: demostrando al juez que las supuestas "irregularidades" no son ediciones maliciosas, sino el comportamiento técnico nativo de un sistema de seguridad no profesional.



NOTICIA DOCTRINAL

TRIBUNAL PERICIAL

EL DIRECTOR DE SEGURIDAD

LA VIDEO VIGILANCIA DOMÉSTICA EN LOS TRIBUNALES

Reto Operativo y Jurídico de las Cámaras IP no Homologadas



4. Directrices para la Valoración Pericial desde la Seguridad Privada

Como miembros de ASPEJURE y auxiliares de la Justicia, proponemos las siguientes máximas para el enjuiciamiento de sistemas de videovigilancia de consumo:

1. **Diferenciar la Limitación Técnica de la Alteración:** Una alteración implica intencionalidad (cortar fotogramas clave, borrar una franja horaria). Una limitación técnica (pixelado, pérdida de audio por AGC o cambio de formato al usar la App) es inherente al diseño del sistema.
2. **Evaluar el Entorno de la Instalación:** Un sistema doméstico conectado por Wi-Fi sufrirá latencias que justifican los saltos temporales de milisegundos en el vídeo. Esto debe explicarse al juzgador como una realidad de las telecomunicaciones, no como un fraude procesal.
3. **Proporcionalidad Operativa:** La prueba debe ser analizada comprendiendo las capacidades reales del equipo instalado, no evaluando una cámara IP de 30 euros con las exigencias de un sistema perimetral de infraestructuras críticas.

5. Conclusión Doctrinal

El avance de los sistemas *Plug & Play* (Internet de las Cosas - IoT) ha borrado la frontera tradicional de la videovigilancia.

La impugnación de evidencias de vídeo no puede basarse en la incomprensión de cómo estos sistemas domésticos gestionan la red, el almacenamiento y la exportación móvil.

Corresponde a los Peritos Judiciales en Dirección de Seguridad Privada, y a los Peritos Judiciales en Informática Forense, siempre alineados con la doctrina de la Sala Segunda del Tribunal Supremo, ilustrar a los tribunales sobre el funcionamiento real de estas tecnologías.

Solo así garantizaremos que la justicia se imparta basándose en la realidad operativa de los sistemas de seguridad, neutralizando impugnaciones artificiosas que pretenden invalidar la verdad material de los hechos grabados.

Firmado por MORENO
MORGADO MANUEL DAVID -
***5381** el día
08/04/2026 con un
certificado emitido

Fdo.: Manuel David Moreno Morgado

Perito Judicial ASPEJURE nº 3157

Director de Seguridad (TIP: 33599)